Abelian Surfaces with Complex Multiplication Admitting Nonprincipal Polarizations

A Dissertation
Presented in Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy
with a
Major in Mathematics
in the
College of Graduate Studies
University of Idaho
by
Jordan Hardy

Approved by:
Major Professor: Jennifer Johnson-Leung, Ph.D.
Committee Members: Brooks Roberts, Ph.D.; Hirotachi Abo, Ph.D.;
Dilshani Sarathchandra, Ph.D
Department Chair: Hirotachi Abo, Ph.D.

August 2023

Abstract

The theory of complex multiplication of abelian varieties is a useful field of study with applications ranging from the explicit construction of abelian extensions CM-fields to the explicit description of L-functions of abelian varieties in ways which are much easier to carry out than the more general case. In the literature the most commonly studied abelian surfaces are those with a principal polarization. In the present thesis we extend this analysis to describe abelian surfaces with complex multiplication which carry a nonprincipal polarization. We provide a complete characterization of which types of polarizations are possible on abelian surfaces which have complex multiplication by a given quartic CM-field K as well as how to construct them when they do exist. We also derive several necessary conditions for such abelian surfaces to exist as well as provide an existence theorem in limited circumstances.

Acknowledgments

I have very many people to thank for my completion of this thesis. I want to thank the members of my committee. I thank Dr. Jennifer Johnson-Leung and Dr. Brooks Roberts for their tireless support of me during the writing process. Without their help, it would certainly not have been possible to write this. I would like to thank Dr. Hirotachi Abo for his support of me during my mathematical education as well as for agreeing to be on my committee. I'd like to thank Dr. Dilshani Sarathchandra for agreeing to be on my committee and for her support and emphasis on making sure the defense process is fair. I would like to thank all my professors for providing the background knowledge necessary for this work. I would like to thank the Department of Mathematics and Statistical Science staff for their incredible work in supporting graduate students for my entire time here.

Dedication

I would like to dedicate this thesis to my family, especially my father Chris Hardy, my sister Erica Jacobs, my brother-in-law Bob Jacobs and my nephew Timothy Jacobs. Their love and support has been important. I'd also like to thank my best friend Anthony St. Claire who has long been a confidant, willing to listen when I need an ear.

Contents

List of Tables

List of Figures

Chapter 1: Introduction

The study of complex multiplication has a rich history, but the idea begins in a relatively familiar place. Consider the study of abelian extensions of the field of rational numbers $\mathbb{Q}$. There is a classical theorem known as the Kronecker-Weber Theorem which states that for every abelian extension K of $\mathbb{Q}$ there exists a natural number n such that $K \subseteq \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. There is a fruitful way to reframe this. Consider the transcendental function $e : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ defined by $x \mapsto e^{2\pi i x}$. Interpreting $\mathbb{R}/\mathbb{Z}$ as the circle group, we note that the n-th roots of unity are the images of n-torsion points under this function. This led Kronecker to ponder the question of whether there were other transcendental functions defined on geometric groups such that the images of torsion points generated abelian extensions of other number fields. To put this in other words, can we generate the class fields of a given number field using special values of such functions?

In at least one special case the answer to this question turns out to be yes, but it takes a little more work to explain the geometric objects which assist us in this setting. Consider an elliptic curve E. Elliptic curves are genus one projective curves with a marked point. Such curves carry a natural group law. Assume that E is defined over a number field, that is, a finite extension of $\mathbb{Q}$. A homomorphism of elliptic curves is a group homomorphism which is a morphism of varieties. The set $\mathrm{End}(E)$ of endomorphisms of E, that is, of homomorphisms from E to itself, forms a ring. For most curves this ring is isomorphic to the integers. In rare circumstances when it is bigger, it is isomorphic to an order $\mathfrak{O}$ contained in a quadratic imaginary field K. E is then said to have complex multiplication by K or by $\mathfrak{O}$. We will also abbreviate "complex multiplication" by CM often. Further, in this case, E tells us about the class field theory of K. The j-invariant is a modular function which parameterizes elliptic curves. Two elliptic curves are isomorphic if and only if their j-invariants are the same, and an elliptic curve is defined over a number field F if and only if its j-invariant is contained in F. The j-invariant serves the same role in generating abelian extensions of quadratic imaginary fields K as the exponential played in the generation of abelian extensions of $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{-m})$ be a quadratic imaginary field where m is a squarefree positive integer. The theory of complex multiplication of elliptic curves has as a major result that if H is the Hilbert class field of a quadratic imaginary field K then H is generated over $K = \mathbb{Q}$ by $j(\omega)$ where

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4, \\ \sqrt{m} & \text{otherwise.} \end{cases}$$

From a geometric point of view this is because there is an elliptic curve isomorphic to

$$E_{\mathfrak{O}_K} = \mathbb{C}/(\mathbb{Z} + \omega\mathbb{Z}) = \mathbb{C}/\mathfrak{O}_K$$

which admits complex multiplication by $\mathfrak{O}_K$. If $h(K)$ is the class number of K then there are $h(K)$ distinct isomorphism classes of elliptic curve with complex multiplication by $\mathfrak{O}_K$ and each of them are the Galois conjugates of $E_{\mathfrak{O}_K}$. Further, their j-invariants are the Galois conjugates of $j(\omega)$.

One can even go beyond this. By replacing ω with a generator of various nonmaximal orders of K, or by replacing j with modular functions for various other congruence subgroups of $SL(2,\mathbb{Z})$ we find generators of abelian extensions of K with nontrivial conductor. In fact, one gets explicit descriptions of every class field over a quadratic imaginary field K using such methods so that the theory of complex multiplication of elliptic curves provides a complete description of the class field theory of quadratic imaginary fields.

The natural next question to consider is whether we get a similar theory when we replace elliptic curves with abelian varieties of higher dimension, while also replacing quadratic imaginary fields with the appropriate number fields which contain rings isomorphic to endomorphism rings of abelian varieties of higher dimension. (These fields are called CM-fields). The answer is, at least in part, no. We do not achieve nearly as complete an explicit description of the class field theory of a higher degree CM-field by means of abelian varieties with complex multiplication. However, in [**13**], Shimura and Taniyama were able to establish partial results to these ends, and while not all class fields of a CM-field K are constructable by means of values of modular functions at CM-points of the Siegel modular variety, they were able to generate some class fields over K using such methods. In particular they proved that if ω is the value of a Siegel modular function whose Fourier coefficients lie in a cyclotomic field on a CM-point corresponding to a CM-field K then ω generates an abelian extension over K. However, there is also a new complication which is introduced when we increase the dimension of the abelian varieties considered.

An abelian variety A is a group variety which admits an embedding into projective space. If such a variety is defined over the complex numbers, its complex points are always isomorphic $\mathbb{C}^g/L$ where g is the dimension of A and L is a lattice in $\mathbb{C}^g$. The existence of such an embedding is equivalent to the existence of a very ample divisor on A, which is in turn equivalent to the existence of a certain $\mathbb{Z}$-bilinear form on L which is called a Riemann form. To each Riemann form E we can associate a tuple $(m_1, \ldots, m_g)$ where g is the dimension of A. We will describe the construction of this tuple later in this thesis. The tuple $(m_1, \ldots, m_g)$ is called the type of the polarization. On the other hand, every lattice L in $\mathbb{C}^g$ is such that $\mathbb{C}^g/L$ is isomorphic to some abelian variety A if and

only if it admits a Riemann form. This detail is not considered for elliptic curves because every lattice L in $\mathbb{C}$ admits a canonical Riemann form. In the higher dimensional case we are free to consider questions of which abelian varieties with complex multiplication by a given order in a CM-field K admit a polarization of a given type. The most commonly considered case is when $m_1 = \cdots = m_g = 1$, in which case the polarization is called a principal polarization. See for instance [**13**] and [**17**].

There has been much less work on nonprincipal polarizations, and the purpose of this thesis is to consider the conditions under which an abelian surface admits a polarization of type (m_1, m_2) for $m_1 > 1$ or $m_2 > 1$. We were able to establish exact conditions under which such an abelian surface exists. Such conditions are very detailed and difficult to check by hand so we have also written an algorithm and implemented it in the PARI programming language in order to quickly ascertain whether for a given CM-field K there exists an abelian surface A with a polarization of type $(1, m)$ whose endomorphism ring is isomorphic to the ring of integers $\mathfrak{O}_K$. We also proved several simpler necessary conditions for such an abelian surface with complex multiplication to exist and proved a sufficient condition for there to exist some abelian surface with a polarization of type $(1, m)$ and with complex multiplication by $\mathfrak{O}_K$ under certain conditions. This makes the theory of these fields more concrete, and we are hopeful that this will open up further avenues to use these surfaces to study the explicit class field theory of quartic CM-fields.

We have access to a good deal of data concerning these results, of which we have only included a small portion in this thesis for illustrative purposes. In addition to illustrating necessary conditions for the existence of certain CM abelian surfaces, this also provides evidence for some observations and conjectures. For instance, for each prime p, there turns out to be empirical evidence that there is a constant α_p between 0 and 1 for which, given a whole number d, the amount of quartic CM-fields of discriminant less than d which admits a polarization of type $(1, p)$ is approximately $\alpha_p d$. This basic pattern has held for every prime we have considered, though we do not have a proof that this always holds yet.

Another pattern which has emerged is that although the theory describes many different sorts of primes p for which there could in principal exist an abelian surface with complex multiplication by a given CM-field K and a polarization of type $(1, p)$, there are certain primes which are not ruled out by our main theorem but for which, nonetheless, we have failed to find examples of such a polarization.

Chapter 2: Some Theory

We begin with some algebraic number theory which will be necessary for proving our main results. Section 2.1 discusses results which apply to a more general setting and the reader may not find them important until they are required for a proof in Chapter 3. Section 2.2 is about the general theory of CM-fields. In Section 2.3 we discuss the basic theory of abelian varieties. In Section 2.4 we discuss a certain class of bilinear forms defined on a CM-field K which will be important in our main theorem. In Section 2.5 we discuss polarizations on abelian varieties.

2.1. Algebraic Prerequisites

Before we do anything else, we will list some algebraic facts relating to field theory which will be useful later. These are lemmas which are used in the proofs of some more technical facts and will seem unmotivated at this time. The reader is advised to move on to the next section and return when the results are needed.

LEMMA 2.1.1. *Let $\mathfrak{O}$ be a Dedekind domain. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be integral ideals of $\mathfrak{O}$. Then we have*

$$\mathfrak{a}^{-1}\mathfrak{b}^{-1}/\mathfrak{c} \simeq \mathfrak{a}^{-1}/\mathfrak{b}\mathfrak{c}$$

where the isomorphism is an isomorphism of $\mathfrak{O}$-modules.

PROOF. First we show that it suffices to prove the claim in the case when $\mathfrak{b}$ is a power of a prime ideal. To show this, let the prime decomposition of $\mathfrak{b}$ be

$$\mathfrak{b} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}.$$

Suppose the claim is true for prime powers. Then we have

$$\begin{aligned}
\mathfrak{a}^{-1}\mathfrak{b}^{-1}/\mathfrak{c} &= \frac{\mathfrak{a}^{-1}\mathfrak{p}_1^{-e_1} \dots \mathfrak{p}_t^{-e_t}}{\mathfrak{c}} \\
&= \frac{\mathfrak{a}^{-1}\mathfrak{p}_1^{-e_1} \dots \mathfrak{p}_{t-1}^{e_{t-1}}}{\mathfrak{p}_n^{e_n}\mathfrak{c}} \\
&= \dots \\
&= \frac{\mathfrak{a}^{-1}}{\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}\mathfrak{c}} \\
&= \frac{\mathfrak{a}^{-1}}{\mathfrak{b}\mathfrak{c}}.
\end{aligned}$$

So, suppose $\mathfrak{b} = \mathfrak{p}^e$ for $\mathfrak{p}$ a prime of $\mathfrak{O}$ and e a positive integer. Let π be an element of $\mathfrak{O}$ whose valuation at $\mathfrak{p}$ is $v_\mathfrak{p}(\pi) = 1$ and such that if $\mathfrak{q}$ is any prime of $\mathfrak{O}$ dividing $\mathfrak{a}$ other than $\mathfrak{p}$ then $v_\mathfrak{q}(\pi) = 0$. Such an element is guaranteed to exist by the approximation

theorem (See [**10**] Theorem 3.4). We define a map $\psi : \mathfrak{a}^{-1}\mathfrak{b}^{-1} \to \mathfrak{a}^{-1}/\mathfrak{bc}$ in the following way.

Let the prime factorization of $\mathfrak{a}$ be

$$\mathfrak{q}_1^{f_1} \dots \mathfrak{q}_s^{f_s}\mathfrak{p}^{f_{s+1}}.$$

Here $f_{s+1} = 0$ if $\mathfrak{p} \nmid \mathfrak{a}$. Then $x \in \mathfrak{a}^{-1}\mathfrak{b}^{-1}$ if and only if $v_\mathfrak{p}(x) \geqslant -f_{s+1} - e$ and $v_{\mathfrak{q}_j}(x) \geqslant f_j$ for each $j \in \{1, \dots, s\}$. Let $x \in \mathfrak{a}^{-1}\mathfrak{b}^{-1}$. We claim that $\pi^e x \in \mathfrak{a}^{-1}$. Indeed, as $v_\mathfrak{p}(x) \geqslant -f_{s+1} - e$, $v_\mathfrak{p}(\pi^e x) \geqslant -f_{s+1}$ and $v_{\mathfrak{q}_j}(\pi^e x) = v_{\mathfrak{q}_j}(x)$ for each $j \in \{1, \dots, s\}$. So $\pi^e x \in \mathfrak{a}^{-1}$. We define $\psi(x) = \pi^e x + \mathfrak{bc}$. We claim $\ker \psi = \mathfrak{c}$. To see this, first suppose $x \in \ker \psi$. So $\psi(x) = \mathfrak{bc}$ or equivalently $\pi^e x \in \mathfrak{bc}$. Then $\mathfrak{bc} | x\mathfrak{p}^e = x\mathfrak{b}$, which implies $\mathfrak{c}|(x)$, which is equivalent to $x \in \mathfrak{c}$. Conversely, if $x \in \mathfrak{c}$ then $\psi(x) + \mathfrak{bc} = \mathfrak{bc}$, so that $x \in \ker \psi$. Therefore by the first isomorphism theorem we have

$$\mathfrak{a}^{-1}\mathfrak{b}^{-1}/\mathfrak{c} \simeq \mathfrak{a}^{-1}/\mathfrak{bc}$$

as required. □

PROPOSITION 2.1.2. *Let $\mathfrak{O}_K$ be the ring of integers of a number field K and $\mathfrak{p}$ a prime ideal of $\mathfrak{O}_K$. Let p be the rational prime lying under $\mathfrak{p}$ and let $e = e(\mathfrak{p}|p)$ and $f = f(\mathfrak{p}|p)$. Let k be a positive integer and let $\widetilde{k}$ denote the least residue of k mod e. Then, as abelian groups,*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-\widetilde{k}}{e}}\mathbb{Z}\right)^{f(e-\widetilde{k})} \times \left(\mathbb{Z}/p^{\frac{k-\widetilde{k}}{e}+1}\mathbb{Z}\right)^{f\widetilde{k}}. \tag{2.1.1}$$

In particular, if $e|k$, we have

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{e}}\mathbb{Z}\right)^{fe}. \tag{2.1.2}$$

PROOF. First, note that we can prove this proposition by proving the analogous proposition where we replace $\mathfrak{O}_K$ by its completion $\mathfrak{O}_\mathfrak{p}$ with respect to the nonarchimedean absolute value corresponding to $\mathfrak{p}$. Let $\mathfrak{O} = \mathfrak{O}_\mathfrak{p}$. We will also refer to the unique maximal ideal of $\mathfrak{O}$ by $\mathfrak{p}$. It is well-known that $\mathfrak{O}_K/\mathfrak{p}^k$ is isomorphic as a ring to $\mathfrak{O}/\mathfrak{p}^k$, so in particular they are also isomorphic as groups. So it suffices to show that $\mathfrak{O}/\mathfrak{p}^k$ has the required form.

Let P be a finite abelian p-group. The fundamental theorem of finite abelian groups tells us that P can be written as a product of cyclic p-groups. In other words, there exist positive integers $n_1, \dots, n_l, r_1, \dots, r_l$ such that

$$P \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z})^{r_1} \times \dots \times (\mathbb{Z}/p^{n_l}\mathbb{Z})^{r_l}.$$

Further, if we define for $n \geqslant 0$

$$U(n, P) = \text{ the number of components of order } p^{n+1}$$

then

$$U(n,P) = \dim \frac{p^n P}{p^{n+1}P} - \dim \frac{p^{n+1}P}{p^{n+2}P}$$

where dim denotes dimension as a $\mathbb{Z}/p\mathbb{Z}$ vector space (see [**11**]). Let $G = \mathfrak{O}/\mathfrak{p}^k$. Then G is a finite abelian p-group.

First, assume that $n \leqslant ke^{-1} - 1$, or equivalently $(n+1)e \leqslant k$. Then

$$\frac{p^n G}{p^{n+1}G} = \frac{\mathfrak{p}^{ne}/\mathfrak{p}^k}{\mathfrak{p}^{(n+1)e}/\mathfrak{p}^k} \simeq \frac{\mathfrak{p}^{ne}}{\mathfrak{p}^{(n+1)e}} \simeq \frac{\mathfrak{O}}{\mathfrak{p}^e}.$$

This has order p^{ef}. So $\dim \frac{p^n G}{p^{n+1}G} = ef$.

Next, assume that $n \geqslant ke^{-1}$ (so that $ne \geqslant k$). In this case, $p^n\mathfrak{O} = \mathfrak{p}^{ne} \subseteq \mathfrak{p}^k$, so $\dim \frac{p^n G}{p^{n+1}G} = 0$.

Finally, assume that $ke^{-1} - 1 < n < ke^{-1}$ so that $ne < k < (n+1)e$. In this case, $p^{n+1}\mathfrak{O} \subsetneq \mathfrak{p}^k \subseteq p^n\mathfrak{O}$. So

$$\frac{p^n G}{p^{n+1}G} = \frac{p^n\mathfrak{O}/\mathfrak{p}^k}{p^{n+1}(\mathfrak{O}/\mathfrak{p}^k)} = \frac{\mathfrak{p}^{ne}}{\mathfrak{p}^k} \simeq \frac{\mathfrak{O}}{\mathfrak{p}^{k-ne}}.$$

So $\dim \frac{p^n G}{p^{n+1}G} = \dim \frac{\mathfrak{O}}{\mathfrak{p}^{k-ne}} = f(k-ne)$.

Putting all this together, we calculate $U(n,G)$ for $n \geqslant 0$:

$$\begin{aligned} U(n,G) &= \dim \frac{p^n G}{p^{n+1}G} - \dim \frac{p^{n+1}G}{p^{n+2}G} \\ &= \begin{cases} 0 & \text{if } n \leqslant ke^{-1} - 2, \\ f(e-k+(n+1)e) & \text{if } ke^{-1} - 2 < n < ke^{-1} - 1, \\ fe & \text{if } n = ke^{-1} - 1, \\ f(k-ne) & \text{if } ke^{-1} - 1 \leqslant n \leqslant ke^{-1}, \\ 0 & \text{if } ke^{-1} \leqslant n. \end{cases} \end{aligned}$$

Assume e divides k. In this case, we have that

$$U(ke^{-1} - 1, G) = fe$$

and $U(n,G) = 0$ otherwise. This implies (2.1.2).

Assume e may not divide k. In this case, we have that

$$U(\left\lfloor ke^{-1} - 1 \right\rfloor, G) = f(e - k + \left\lfloor ke^{-1} \right\rfloor e),$$

$$U(\left\lfloor ke^{-1} \right\rfloor, G) = f(k - \left\lfloor ke^{-1} \right\rfloor e)$$

and $U(n,G) = 0$ otherwise. A calculation now gives us (2.1.1). □

This gives us the tool to compute what quotients of rings of integers by ideals look like in various fields. Most important in this document will be the case of quartic fields. We have the following lemma.

LEMMA 2.1.3. *Let K be a quartic field. Let $\mathfrak{O}_K$ be the ring of integers of K. Let k be a positive integer. Let $\mathfrak{p}$ be a prime in $\mathfrak{O}_K$ lying over a rational prime p. Let $e = e(\mathfrak{p}|p)$ be the ramification degree of $\mathfrak{p}$ and $f = f(\mathfrak{p}|p)$ the inertia degree of $\mathfrak{p}$. Because $[K : \mathbb{Q}] = 4$ we have the following possibilities for e, f which result in the following isomorphisms of abelian groups.*

(1) *Assume $e = 4, f = 1$. Then:*
   (a) *If $k \equiv 0 \pmod 4$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{4}}\mathbb{Z}\right)^4;$$
   (b) *If $k \equiv 1 \pmod 4$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{4}}\mathbb{Z}\right)^3 \times \mathbb{Z}/p^{\frac{k-1}{4}+1}\mathbb{Z};$$
   (c) *If $k \equiv 2 \pmod 4$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{4}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-2}{4}+1}\mathbb{Z}\right)^2;$$
   (d) *If $k \equiv 3 \pmod 4$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-3}{4}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-3}{4}+1}\mathbb{Z}\right)^3.$$
(2) *Assume $e = 3, f = 1$. Then:*
   (a) *If $k \equiv 0 \pmod 3$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{3}}\mathbb{Z}\right)^3;$$
   (b) *If $k \equiv 1 \pmod 3$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{3}}\mathbb{Z}\right)^2 \times \mathbb{Z}/p^{\frac{k-1}{3}+1}\mathbb{Z};$$
   (c) *If $k \equiv 2 \pmod 3$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-2}{3}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-2}{3}+1}\mathbb{Z}\right)^2.$$
(3) *Assume $e = 2, f = 2$. Then:*
   (a) *If $k \equiv 0 \pmod 2$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^4;$$
   (b) *If $k \equiv 1 \pmod 2$*
   $$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}\right)^2.$$
(4) *Assume $e = 2, f = 1$. Then:*

(a) *If* $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^2;$$

(b) *If* $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z} \times \mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}.$$

(5) *Assume* $e = 1, f = 4$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4.$$

(6) *Assume* $e = 1, f = 3$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^3.$$

(7) *Assume* $e = 1, f = 2$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^2.$$

(8) *Assume* $e = 1, f = 1$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^k\mathbb{Z}.$$

Proof. This is a direct application of the Proposition 2.1.2. □

We also carry out the same calculations for sextic and octic fields.

Theorem 2.1.4. *Let* K *be a sextic field. Let* $\mathfrak{O}_K$ *be the ring of integers of* K *and* $\mathfrak{p}$ *a prime of* $\mathfrak{O}_K$. *Let* p *be the rational prime lying below* $\mathfrak{p}$. *Let* k *be a positive integer. Let* $e = e(\mathfrak{p}|p)$ *be the ramification degree of* $\mathfrak{p}$ *and* $f = f(\mathfrak{p}|p)$ *the inertia degree of* $\mathfrak{p}$. *We have the following possibilities for* e *and* f *and the corresponding group structures for* $\mathfrak{O}_K/\mathfrak{p}^k$.

(1) *Assume* $e = 6, f = 1$. *Then:*

(a) *If* $k \equiv 0 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{6}}\mathbb{Z}\right)^6;$$

(b) *If* $k \equiv 1 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{6}}\mathbb{Z}\right)^5 \times \mathbb{Z}/p^{\frac{k-1}{6}+1}\mathbb{Z};$$

(c) *If* $k \equiv 2 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{6}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-2}{6}+1}\mathbb{Z}\right)^2;$$

(d) *If* $k \equiv 3 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{6}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-3}{6}+1}\mathbb{Z}\right)^3;$$

(e) *If* $k \equiv 4 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-4}{6}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-4}{6}+1}\mathbb{Z}\right)^4;$$

(f) *If* $k \equiv 5 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-5}{6}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-5}{6}+1}\mathbb{Z}\right)^5.$$

(2) *Assume* $e = 5, f = 1$. *Then:*

(a) *If* $k \equiv 0 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{5}}\mathbb{Z}\right)^5;$$

(b) *If* $k \equiv 1 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{5}}\mathbb{Z}\right)^4 \times \mathbb{Z}/p^{\frac{k-1}{5}+1}\mathbb{Z};$$

(c) *If* $k \equiv 2 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{5}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-2}{5}+1}\mathbb{Z}\right)^2;$$

(d) *If* $k \equiv 3 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{5}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-3}{5}+1}\mathbb{Z}\right)^3;$$

(e) *If* $k \equiv 4 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-4}{5}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-4}{5}+1}\mathbb{Z}\right)^4.$$

(3) *Assume* $e = 4, f = 1$. *Then:*

(a) *If* $k \equiv 0 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{4}}\mathbb{Z}\right)^4;$$

(b) *If* $k \equiv 1 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{4}}\mathbb{Z}\right)^3 \times \mathbb{Z}/p^{\frac{k-1}{4}+1}\mathbb{Z};$$

(c) *If* $k \equiv 2 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{4}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-2}{4}+1}\mathbb{Z}\right)^2;$$

(d) *If* $k \equiv 3 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-3}{4}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-3}{4}+1}\mathbb{Z}\right)^3.$$

(4) *Assume* $e = 3, f = 2$. *Then:*

(a) *If* $k \equiv 0 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{3}}\mathbb{Z}\right)^6;$$

(b) *If* $k \equiv 1 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{3}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-1}{3}+1}\mathbb{Z}\right)^2;$$

(c) *If* $k \equiv 2 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{3}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-2}{3}+1}\mathbb{Z}\right)^4.$$

(5) *Assume* $e = 3, f = 1$. *Then:*

(a) *If* $k \equiv 0 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{3}}\mathbb{Z}\right)^3;$$

(b) *If* $k \equiv 1 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{3}}\mathbb{Z}\right)^2 \times \mathbb{Z}/p^{\frac{k-1}{3}+1}\mathbb{Z};$$

(c) *If* $k \equiv 2 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-2}{3}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-2}{3}+1}\mathbb{Z}\right)^2.$$

(6) *Assume* $e = 2, f = 3$, *Then:*

(a) *If* $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^6;$$

(b) *If* $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}\right)^3.$$

(7) *Assume* $e = 2, f = 2$. *Then:*

(a) *If* $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^4;$$

(b) *If* $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}\right)^2.$$

(8) *Assume* $e = 2, f = 1$. *Then:*

(a) *If* $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^2;$$

(b) *If* $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z} \times \mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}.$$

(9) *Assume* $e = 1, f = 6$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^6.$$

(10) *Assume* $e = 1, f = 5$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^5.$$

(11) *Assume* $e = 1, f = 4$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4.$$

(12) *Assume* $e = 1, f = 3$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^3.$$

(13) *Assume* $e = 1, f = 2$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^2.$$

(14) *Assume* $e = 1, f = 1$. *Then*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^k\mathbb{Z}.$$

THEOREM 2.1.5. *Let* K *be an octic field. Let* $\mathfrak{O}_K$ *be the ring of integers of* K *and* $\mathfrak{p}$ *a prime of* $\mathfrak{O}_K$. *Let* p *be the rational prime lying below* $\mathfrak{p}$. *Let* k *be a positive integer. Let* $e = e(\mathfrak{p}|p)$ *be the ramification degree of* $\mathfrak{p}$ *and* $f = f(\mathfrak{p}|p)$ *the inertia degree of* $\mathfrak{p}$. *We have the following possibilities for* e *and* f *and the corresponding group structures for* $\mathfrak{O}_K/\mathfrak{p}^k$.

(1) *Assume* $e = 8, f = 1$. *Then:*

(a) *If* $k \equiv 0 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{8}}\mathbb{Z}\right)^8;$$

(b) *If* $k \equiv 1 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{8}}\mathbb{Z}\right)^7 \times \mathbb{Z}/p^{\frac{k-1}{8}+1}\mathbb{Z};$$

(c) $k \equiv 2 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{8}}\mathbb{Z}\right)^6 \times \left(\mathbb{Z}/p^{\frac{k-2}{8}+1}\mathbb{Z}\right)^2;$$

(d) $k \equiv 3 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{8}}\mathbb{Z}\right)^5 \times \left(\mathbb{Z}/p^{\frac{k-3}{8}+1}\mathbb{Z}\right)^3;$$

(e) $k \equiv 4 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-4}{8}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-4}{8}+1}\mathbb{Z}\right)^4;$$

(f) $k \equiv 5 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-5}{8}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-5}{8}+1}\mathbb{Z}\right)^5;$$

(g) $k \equiv 6 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-6}{8}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-6}{8}+1}\mathbb{Z}\right)^6;$$

(h) $k \equiv 7 \pmod 8$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-7}{8}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-7}{8}+1}\mathbb{Z}\right)^7.$$

(2) *Assume* $e = 7, f = 1$. *Then:*

(a) $k \equiv 0 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{7}}\mathbb{Z}\right)^7;$$

(b) $k \equiv 1 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{7}}\mathbb{Z}\right)^5 \times \mathbb{Z}/p^{\frac{k-1}{7}+1}\mathbb{Z};$$

(c) $k \equiv 2 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{7}}\mathbb{Z}\right)^5 \times \left(\mathbb{Z}/p^{\frac{k-2}{7}+1}\mathbb{Z}\right)^2;;$$

(d) $k \equiv 3 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{7}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-3}{7}+1}\mathbb{Z}\right)^3;;$$

(e) $k \equiv 4 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-4}{7}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-4}{7}+1}\mathbb{Z}\right)^4;$$

(f) $k \equiv 5 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-5}{7}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-5}{7}+1}\mathbb{Z}\right)^5;$$

(g) $k \equiv 6 \pmod 7$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-6}{7}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-6}{7}+1}\mathbb{Z}\right)^6.$$

(3) *Assume* $e = 6, f = 1$. *Then:*

(a) $k \equiv 0 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{6}}\mathbb{Z}\right)^6;$$

(b) $k \equiv 1 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{6}}\mathbb{Z}\right)^5 \times \mathbb{Z}/p^{\frac{k-1}{6}+1}\mathbb{Z};$$

(c) $k \equiv 2 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{6}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-2}{6}+1}\mathbb{Z}\right)^2 .;$$

(d) $k \equiv 3 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{6}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-3}{6}+1}\mathbb{Z}\right)^3 .;$$

(e) $k \equiv 4 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-4}{6}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-4}{6}+1}\mathbb{Z}\right)^4 ;$$

(f) $k \equiv 5 \pmod 6$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-5}{6}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-5}{6}+1}\mathbb{Z}\right)^5 .$$

(4) *Assume* $e = 5, f = 1$. *Then:*

(a) $k \equiv 0 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{5}}\mathbb{Z}\right)^5 ;$$

(b) $k \equiv 1 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{5}}\mathbb{Z}\right)^4 \times \mathbb{Z}/p^{\frac{k-1}{5}+1}\mathbb{Z};$$

(c) $k \equiv 2 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{5}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-2}{5}+1}\mathbb{Z}\right)^2 ;$$

(d) $k \equiv 3 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{5}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-3}{5}+1}\mathbb{Z}\right)^3 ;$$

(e) $k \equiv 4 \pmod 5$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-4}{5}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-4}{5}+1}\mathbb{Z}\right)^4 .$$

(5) *Assume* $e = 4, f = 2$. *Then:*

(a) $k \equiv 0 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{4}}\mathbb{Z}\right)^8 ;$$

(b) $k \equiv 1 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{4}}\mathbb{Z}\right)^6 \times \left(\mathbb{Z}/p^{\frac{k-1}{4}+1}\mathbb{Z}\right)^2 ;$$

(c) $k \equiv 2 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{4}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-2}{4}+1}\mathbb{Z}\right)^4;$$

(d) $k \equiv 3 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-3}{4}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-3}{4}+1}\mathbb{Z}\right)^6.$$

(6) *Assume* $e = 4, f = 1$. *Then:*

(a) $k \equiv 0 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{4}}\mathbb{Z}\right)^4;$$

(b) $k \equiv 1 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{4}}\mathbb{Z}\right)^3 \times \mathbb{Z}/p^{\frac{k-1}{4}+1}\mathbb{Z};$$

(c) $k \equiv 2 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{4}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-2}{4}+1}\mathbb{Z}\right)^2;$$

(d) $k \equiv 3 \pmod 4$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-3}{4}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-3}{4}+1}\mathbb{Z}\right)^3.$$

(7) *Assume* $e = 3, f = 2$. *Then:*

(a) $k \equiv 0 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{3}}\mathbb{Z}\right)^6;$$

(b) $k \equiv 1 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{3}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-1}{3}+1}\mathbb{Z}\right)^2;$$

(c) $k \equiv 2 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-2}{3}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-2}{3}+1}\mathbb{Z}\right)^4.$$

(8) *Assume* $e = 3, f = 1$. *Then:*

(a) $k \equiv 0 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{3}}\mathbb{Z}\right)^3;$$

(b) $k \equiv 1 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{3}}\mathbb{Z}\right)^2 \times \mathbb{Z}/p^{\frac{k-1}{3}+1}\mathbb{Z};$$

(c) $k \equiv 2 \pmod 3$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-2}{3}}\mathbb{Z} \times \left(\mathbb{Z}/p^{\frac{k-2}{3}+1}\mathbb{Z}\right)^2.$$

(9) *Assume* $e = 2, f = 4$. *Then:*

(a) $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^8;$$

(b) $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z}\right)^4 \times \left(\mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}\right)^4.$$

(10) *Assume* $e = 2, f = 3$. *Then:*

(a) $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^6;$$

(b) $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}\right)^3.$$

(11) *Assume* $e = 2, f = 2$. *Then:*

(a) $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^4;$$

(b) $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}\right)^2.$$

(12) *Assume* $e = 2, f = 1$. *Then:*

(a) $k \equiv 0 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{\frac{k}{2}}\mathbb{Z}\right)^2;$$

(b) $k \equiv 1 \pmod 2$

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^{\frac{k-1}{2}}\mathbb{Z} \times \mathbb{Z}/p^{\frac{k-1}{2}+1}\mathbb{Z}.$$

(13) *Assume* $e = 1, f = 8$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^8.$$

(14) *Assume* $e = 1, f = 7$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^7.$$

(15) *Assume* $e = 1, f = 6$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^6.$$

(16) *Assume* $e = 1, f = 5$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^5.$$

(17) *Assume* $e = 1, f = 4$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^4.$$

(18) *Assume* $e = 1, f = 3$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^3.$$

(19) *Assume* $e = 1, f = 2$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^k\mathbb{Z}\right)^2.$$

(20) *Assume* $e = 1, f = 1$. *Then:*

$$\mathfrak{O}_K/\mathfrak{p}^k \simeq \mathbb{Z}/p^k\mathbb{Z}.$$

Having given the abelian group structure of quotients of rings of integers, we now lay out the circumstances under which they take on a certain form which will be important in the proof of the main theorem of this thesis. Specifically we want to find ideals $\mathfrak{g}$ such that $\mathfrak{O}_K/\mathfrak{g}$ is isomorphic to a product of n copies of $\mathbb{Z}/m\mathbb{Z}$.

LEMMA 2.1.6. *Let K be a number field, let $\mathfrak{O}_K$ be the ring of integers of K, let $\mathfrak{g}$ be an ideal of $\mathfrak{O}_K$, and let m and n be positive integers. Assume that*

$$\mathfrak{O}_K/\mathfrak{g} \cong \underbrace{\mathbb{Z}/m\mathbb{Z} \times \cdots \times \mathbb{Z}/m\mathbb{Z}}_{n}. \tag{2.1.3}$$

(1) *If $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$ that divides $\mathfrak{g}$, and $\mathfrak{p}$ lies over the prime p of $\mathbb{Z}$, then $p \mid m$.*

(2) *For each prime p of $\mathbb{Z}$ such that $p \mid m$, define*

$$\mathfrak{g}_p = \prod_{\substack{\mathfrak{p} \text{ is a prime of } \mathfrak{O}_K, \\ \mathfrak{p} \mid \mathfrak{g}, \\ \mathfrak{p} \text{ lies over } p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{g})}. \tag{2.1.4}$$

Then

$$\mathfrak{g} = \prod_{p \mid m} \mathfrak{g}_p \tag{2.1.5}$$

and

$$\mathfrak{O}_K/\mathfrak{g}_p \cong \underbrace{\mathbb{Z}/p^{v_p(m)}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{v_p(m)}\mathbb{Z}}_{n}. \tag{2.1.6}$$

PROOF. Let $m = p_1^{j_1} \cdots p_r^{j_r}$ be the prime factorization of m, and let $\mathfrak{g} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_s^{k_s}$ be the prime factorization of $\mathfrak{g}$. For $i \in \{1, \ldots, s\}$, let $\mathfrak{p}_i$ lie over the prime q_i of $\mathbb{Z}$. By the

Chinese remainder theorem we have

$$\mathfrak{O}_K/\mathfrak{g} \cong \mathfrak{O}_K/\mathfrak{p}_1^{k_1} \times \cdots \times \mathfrak{O}_K/\mathfrak{p}_s^{k_s}. \tag{2.1.7}$$

For this, note that $\mathfrak{p}_i^{k_i}$ and $\mathfrak{p}_j^{k_j}$ are comaximal for $i, j \in \{1, \ldots, s\}$ with $i \neq j$. It follows that

$$|\mathfrak{O}_K/\mathfrak{g}| = q_1^{k_1 f(\mathfrak{p}_1/q_1)} \cdots q_s^{k_s f(\mathfrak{p}_s/q_s)}. \tag{2.1.8}$$

Since (2.1.3) holds we also have

$$|\mathfrak{O}_K/\mathfrak{g}| = m^n = p_1^{nk_1} \cdots p_r^{nk_r}. \tag{2.1.9}$$

From (2.1.8) and (2.1.9) we conclude that $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$. The assertion (1) follows, and (2.1.5) is also clear. To prove (2.1.6) we will use the following notation: if G is a finite abelian group, and p is a prime of $\mathbb{Z}$, then we let G_p be the subgroup of G of elements that have order that is a non-negative power of p. Now by the Chinese remainder theorem from (2.1.5) we have

$$\mathfrak{O}_K/\mathfrak{g} \cong \mathfrak{O}_K/\mathfrak{g}_{p_1} \times \cdots \times \mathfrak{O}_K/\mathfrak{g}_{p_r}. \tag{2.1.10}$$

Let $i \in \{1, \ldots, r\}$. Considering the definition of $\mathfrak{g}_{p_i}$, and applying the Chinese remainder theorem to $\mathfrak{O}_K/\mathfrak{g}_{p_i}$, we see that every element of $\mathfrak{O}_K/\mathfrak{g}_{p_i}$ has order that is a non-negative power of p_i. It follows that

$$(\mathfrak{O}_K/\mathfrak{g})_{p_i} \cong \mathfrak{O}_K/\mathfrak{g}_{p_i}. \tag{2.1.11}$$

It is also evident that

$$\left(\underbrace{\mathbb{Z}/p^m\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}}_{n}\right)_{p_i} \cong \underbrace{\mathbb{Z}/p_i^{v_{p_i}(m)}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i^{v_{p_i}(m)}\mathbb{Z}}_{n}. \tag{2.1.12}$$

We now see that (2.1.6) follows from (2.1.3), (2.1.11), and (2.1.12). □

We now further specialize Lemma 2.1.6 to apply in the specific case K is quartic, when $n = 2$ and $m = p^g$ for a prime p and a positive integer g. This is the specific case which will be useful to us.

LEMMA 2.1.7. *Let K be quartic extension of $\mathbb{Q}$, let $\mathfrak{O}_K$ be the ring of integers of K, let p be a prime of $\mathbb{Z}$, let $\mathfrak{g}$ be an ideal of $\mathfrak{O}_K$, and let g be a positive integer. Assume that*

$$\mathfrak{O}_K/\mathfrak{g} \cong \mathbb{Z}/p^g\mathbb{Z} \times \mathbb{Z}/p^g\mathbb{Z}. \tag{2.1.13}$$

Let

$$\mathfrak{g} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_t^{k_t}, \qquad k_1 \leqslant \cdots \leqslant k_t \tag{2.1.14}$$

be the prime factorization of $\mathfrak{g}$ *(note that* $\mathfrak{g}$ *is a proper ideal of* $\mathfrak{O}_K$*). For* $i \in \{1, \dots, t\}$ *let* $\mathfrak{p}_i$ *lie over the prime* p_i *of* $\mathbb{Z}$*. Then* $p_1 = \cdots = p_t = p$ *and* $\mathfrak{g}$ *and* g *satisfy exactly one of the following conditions:*

(2.1.15)

t	g	$k_1, \dots, k_t$	$(e(\mathfrak{p}_1/p), f(\mathfrak{p}_1/p)), \dots, (e(\mathfrak{p}_t/p), f(\mathfrak{p}_t/p))$
1	1	2	$(4,1)$
1	1	2	$(3,1)$
1	1	1	$(2,2)$
1	g	$2g$	$(2,1)$
1	g	g	$(1,2)$
2	1	$1,1$	$(3,1),(1,1)$
2	1	$1,1$	$(2,1),(2,1)$
2	1	$1,1$	$(2,1),(1,1)$
2	g	g,g	$(1,1),(1,1)$

If $K/\mathbb{Q}$ *is Galois, then* $\mathfrak{g}$ *and* g *satisfy exactly one of the following conditions:*

(2.1.16)

t	g	$k_1, \dots, k_t$	$(e(\mathfrak{p}_1/p), f(\mathfrak{p}_1/p)), \dots, (e(\mathfrak{p}_t/p), f(\mathfrak{p}_t/p))$
1	1	2	$(4,1)$
1	1	1	$(2,2)$
1	g	$2g$	$(2,1)$
1	g	g	$(1,2)$
2	1	$1,1$	$(2,1),(2,1)$
2	g	g,g	$(1,1),(1,1)$

PROOF. By the Chinese remainder theorem we have

$$\mathfrak{O}_K/\mathfrak{g} \cong \mathfrak{O}_K/\mathfrak{p}_1^{k_1} \times \cdots \times \mathfrak{O}_K/\mathfrak{p}_t^{k_t}. \tag{2.1.17}$$

For this, note that $\mathfrak{p}_i^{k_i}$ and $\mathfrak{p}_j^{k_j}$ are comaximal for $i, j \in \{1, \dots, t\}$ with $i \neq j$. For $i \in \{1, \dots, t\}$ we have

$$|\mathfrak{O}_K/\mathfrak{p}_i^{k_i}| = p_i^{f(\mathfrak{p}_i/p_i)k_i}, \tag{2.1.18}$$

so that by (2.1.13),

$$p^{2g} = p_1^{f(\mathfrak{p}_1/p_1)k_1} \cdots p_t^{f(\mathfrak{p}_t/p_t)k_t}. \tag{2.1.19}$$

It follows that $p_1 = \cdots = p_t$ and

$$2g = f(\mathfrak{p}_1/p_1)k_1 + \cdots f(\mathfrak{p}_t/p_t)k_t. \tag{2.1.20}$$

Also, since the factorization of a finite abelian group as a direct product of cyclic groups of prime power order is unique (this is the fundamental theorem of abelian groups), we see that $t = 1$ or $t = 2$.

Assume first that $t = 1$. Then exactly one of first five entries of (2.1.15) holds by the following table (which follows from 3.1.2).

case from 3.1.2	$e(\mathfrak{p}_1/p)$	$f(\mathfrak{p}_1/p)$	k_1	exact conditions such that $\mathfrak{O}_K/\mathfrak{p}_1^{k_1} \cong \mathbb{Z}/p^g\mathbb{Z} \times \mathbb{Z}/p^g\mathbb{Z}$
(1) (a)	4	1	$k_1 \equiv 0 \pmod 4$	impossible
(1) (b)	4	1	$k_1 \equiv 1 \pmod 4$	impossible
(1) (c)	4	1	$k_1 \equiv 2 \pmod 4$	$k_1 = 2$ and $g = 1$
(1) (d)	4	1	$k_1 \equiv 3 \pmod 4$	impossible
(2) (a)	3	1	$k_1 \equiv 0 \pmod 3$	impossible
(2) (b)	3	1	$k_1 \equiv 1 \pmod 3$	impossible
(2) (c)	3	1	$k_1 \equiv 2 \pmod 3$	$k_1 = 2$ and $g = 1$
(3) (a)	2	2	$k_1 \equiv 0 \pmod 2$	impossible
(3) (b)	2	2	$k_1 \equiv 1 \pmod 2$	$k_1 = 1$ and $g = 1$
(4) (a)	2	1	$k_1 \equiv 0 \pmod 2$	$2g = k_1$
(4) (b)	2	1	$k_1 \equiv 1 \pmod 2$	impossible
(5)	1	4		impossible
(6)	1	3		impossible
(7)	1	2		$k_1 = g$
(8)	1	1		impossible

Now assume that $t = 2$. Then exactly one of the last four entries of (2.1.15) holds by the following table (which follows from 3.1.2). In the following table $i \in \{1, 2\}$. Note

that since $t = 2$ we must have $\mathfrak{O}_K/\mathfrak{p}_i^{k_i} \cong \mathbb{Z}/p^g\mathbb{Z}$. Note also that we use that

$$4 \geqslant e(\mathfrak{p}_1/p)f(\mathfrak{p}_1/p) + e(\mathfrak{p}_2/p)f(\mathfrak{p}_2/p). \tag{2.1.21}$$

case from Theorem 3.1.2	$e(\mathfrak{p}_i/p)$	$f(\mathfrak{p}_i/p)$	k_i	exact conditions such that $\mathfrak{O}_K/\mathfrak{p}_i^{k_i} \cong \mathbb{Z}/p^g\mathbb{Z}$
(1) (a)	4	1	$k_i \equiv 0 \pmod 4$	impossible
(1) (b)	4	1	$k_i \equiv 1 \pmod 4$	$k_i = g = 1$
(1) (c)	4	1	$k_i \equiv 2 \pmod 4$	impossible
(1) (d)	4	1	$k_i \equiv 3 \pmod 4$	impossible
(2) (a)	3	1	$k_i \equiv 0 \pmod 3$	impossible
(2) (b)	3	1	$k_i \equiv 1 \pmod 3$	$k_i = g = 1$
(2) (c)	3	1	$k_i \equiv 2 \pmod 3$	impossible
(3) (a)	2	2	$k_i \equiv 0 \pmod 2$	impossible
(3) (b)	2	2	$k_i \equiv 1 \pmod 2$	impossible
(4) (a)	2	1	$k_i \equiv 0 \pmod 2$	impossible
(4) (b)	2	1	$k_i \equiv 1 \pmod 2$	$k_i = g = 1$
(5)	1	4		impossible
(6)	1	3		impossible
(7)	1	2		impossible
(8)	1	1		$k_i = g = 1$

Finally, assume that $K/\mathbb{Q}$ is Galois. Then $\mathfrak{g}$ and g cannot satisfy the second, sixth, and eigth entries of (2.1.15) because $e(\mathfrak{p}_i/p)$ divides 4 for $i \in \{1, \ldots, t\}$ and $e(\mathfrak{p}_1/p) = \cdots = e(\mathfrak{p}_t/p)$. □

2.2. CM-Fields

In this section we study a certain generalization of a quadratic imaginary field called a CM-field. These fields arise as the field of fractions of endomorphism rings of some abelian varieties so they will form a central object of study in this thesis. We will need a couple preliminary concepts in order to define a CM-field.

We call a number field K totally imaginary if no embedding of K into the complex numbers takes K into the real numbers. We call K totally real if every embedding of K into the complex numbers takes K into the real numbers. We call an element x of K totally positive or totally negative if every embedding of K into the complex numbers takes x into the positive or negative real numbers respectively.

Definition 2.2.1. A CM-field K is a finite algebraic extension of the field of rational numbers $\mathbb{Q}$ that is totally imaginary and such that K has an index two subextension K_0 which is totally real.

The simplest example of a CM-field is a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-d})$ with d a positive integer. In this case, the totally real subfield is $\mathbb{Q}$. In general, every CM-field is of the form $K = K_0(\sqrt{-\Delta})$ where Δ is some totally positive element of K_0. We begin by proving some basic facts about CM-fields.

Lemma 2.2.2. *Let K be a CM-field. There exists a unique automorphism $\beta : K \to K$ such that*

$$\sigma(\beta(x)) = \overline{\sigma(x)} \qquad \text{for } x \in K \tag{2.2.1}$$

for any embedding $\sigma : K \to \mathbb{C}$. In fact, if K_0 is a totally real subfield of K such that $K = K_0(\sqrt{-\Delta})$ where $\Delta \in K_0$ is totally positive, then

$$\beta(a + b\sqrt{-\Delta}) = a - b\sqrt{-\Delta} \qquad \text{for } a, b \in K_0. \tag{2.2.2}$$

Proof. Let K_0 be a totally real subfield of K such that $K = K_0(\sqrt{-\Delta})$ where $\Delta \in K_0$ is totally positive. Let $\sigma : K \to \mathbb{C}$ be an embedding. We first prove that

$$\overline{\sigma(a + b\sqrt{-\Delta})} = \sigma(a - b\sqrt{\Delta}) \qquad \text{for } a, b \in K_0. \tag{2.2.3}$$

Let $a, b \in K_0$. Then

$$\begin{aligned} \overline{\sigma(a + b\sqrt{-\Delta})} &= \overline{\sigma(a)} + \overline{\sigma(b)}\sigma(\sqrt{-\Delta}) \\ &= \sigma(a) + \sigma(b)\overline{\sigma(\sqrt{-\Delta})}. \end{aligned} \tag{2.2.4}$$

Now

$$\begin{aligned} (\sigma(\sqrt{-\Delta}))^2 &= \sigma(\sqrt{-\Delta}^2) \\ &= \sigma(-\Delta) \\ &= -\sigma(\Delta). \end{aligned}$$

Since Δ is totally positive we have $\sigma(\Delta) > 0$. It follows that

$$\sigma(\sqrt{-\Delta}) = \epsilon_\sigma \sqrt{\sigma(\Delta)} i$$

for some $\epsilon_\sigma \in \{\pm 1\}$. Therefore

$$\begin{aligned}\overline{\sigma(\sqrt{-\Delta})} &= \overline{\epsilon_\sigma \sqrt{\sigma(\Delta)} i} \\ &= -\epsilon_\sigma \sqrt{-\Delta} i \\ &= -\sigma(\sqrt{-\Delta}). \end{aligned} \tag{2.2.5}$$

From (2.2.4) and (2.2.5) we now have

$$\begin{aligned}\overline{\sigma(a + b\sqrt{-\Delta})} &= \sigma(a) - \sigma(b)\sigma(\sqrt{-\Delta}) \\ &= \sigma(a - b\sqrt{-\Delta}).\end{aligned}$$

This proves (2.2.3).

Now define $\beta : K \to K$ by (2.2.2). Then it is clear that β is in $\mathrm{Gal}(K/K_0)$ and in particular β is an automorphism of K. That β satisfies (2.2.1) for any embedding $\sigma : K \to \mathbb{C}$ follows from (2.2.4). Assume $\beta' : K \to K$ is another automorphism that satisfies (2.2.1) with β' in place of β for all embeddings $\sigma : K \to \mathbb{C}$. To complete the proof we need to prove that $\beta' = \beta$. Let $x \in K$. Let $\sigma : K \to \mathbb{C}$ be any embedding. Then $\beta'(x) = \sigma^{-1}(\sigma(\overline{\sigma}(x)) = \beta(x)$. □

This gives us a new characterization of CM-fields

Lemma 2.2.3. *Let K be a number field. The following are equivalent.*

1. *The field K is totally real or a CM-field*
2. *Let $\rho : \mathbb{C} \to \mathbb{C}$ be complex conjugation. There exists an automorphism τ from K to K such that for every embedding $\sigma : K \to \mathbb{C}$, $\rho \circ \sigma = \sigma \circ \tau$.*

Proof. We first prove the forward implication. If K is totally real, the result is trivial. If K is a CM-field, We let $\tau = \beta$ be the automorphism of K from Lemma 2.2.2. Then Lemma 2.2.2 implies (2).

We now prove the converse. Suppose that there exists an automorphism $\tau : K \to K$ such that $\rho \circ \sigma = \sigma \circ \tau$ for every embedding $\sigma : K \to \mathbb{C}$. Let K_0 be the fixed field of τ. If $K = K_0$ then K is totally real. Suppose $K \neq K_0$. Then τ is not the identity. I claim the order of τ is 2. Indeed, if $x \in K$ and $\sigma : K \to \mathbb{C}$ is any embedding of K into $\mathbb{C}$, let τ_K and σ_K be extensions of τ and σ respectively to automorphisms of $\mathbb{C}$. Then we have

$$\begin{aligned}\tau_K^2(x) &= \sigma_K^{-1} \circ \rho \circ \sigma_K \sigma_K^{-1} \circ \rho \circ \sigma_K \\ &= \sigma_K^{-1} \circ \rho^2 \circ \sigma_K \\ &= \mathrm{Id}_{\mathbb{C}}.\end{aligned}$$

Because an extension of τ has order 2, so does τ. K must be a degree two extension of K_0 which is not embedded into the real numbers, thus K is a CM-field. □

We also have the following.

LEMMA 2.2.4. *The following hold.*

(1) *Any composite of finitely many CM-fields and totally real fields is a CM-field or totally real.*
(2) *The Galois closure of a CM-field is a CM-field.*
(3) *If ϕ is an embedding of CM-fields $K_1 \to K_2$, then we have $\rho|_{K_2} \circ \phi = \phi \circ \rho|_{K_1}$.*

PROOF. We start by proving (1). If we can prove the result for two fields K, L then the result will follow in general by induction. Let σ be an embedding of LM into $\mathbb{C}$ and let ρ be complex conjugation. We know that for any $x \in L$ or $x \in M$,

$$\sigma(\rho(x)) = \rho(\sigma(x)).$$

Now let $y \in LM$. Since y can be written as a rational expression of elements of M with coefficients in L, $\sigma(\rho(y) = \rho(\sigma(y))$. (2) is true because the Galois closure of a number field is the composite of the finitely many Galois conjugates of the number field. We prove (3). Note that as $K_2 \subseteq \mathbb{C}$, we can regard the embedding of K_1 into K_2 as an embedding into $\mathbb{C}$, so this result is immediate. □

CM-types. Let K be a CM-field of degree $2g$ over $\mathbb{Q}$.

DEFINITION 2.2.5. A CM-type of K is a collection

$$\Phi = \{\phi_1, \phi_2, \ldots, \phi_g\}$$

of embeddings of K into $\mathbb{C}$ such that $\{\phi_1, \phi_2, \ldots, \phi_g, \phi_1 \circ \rho, \phi_2 \circ \rho, \ldots, \phi_g \circ \rho\}$ is the full set of embeddings of K into $\mathbb{C}$.

Let $M(g, \mathbb{C})$ denote the ring of $g \times g$ matrices with complex entries. Let $D(g, \mathbb{C})$ denote the subring of diagonal matrices. We will abuse notation and also write $\mathbb{C}^g$ for $D(g, \mathbb{C})$.

By abuse of notation, we also use Φ to denote the map $K \to D(g, \mathbb{C})$ defined by

$$\Phi(x) = \begin{pmatrix} \phi_1(x) & & \\ & \ddots & \\ & & \phi_g(x) \end{pmatrix}. \tag{2.2.6}$$

Note that as we are associating $D(g, \mathbb{C})$ with $\mathbb{C}^g$ we might also write this as a row vector:

$$\Phi(x) = (\phi_1(x), \ldots, \phi_g(x)).$$

However, because $\Phi(x)$ for each $x \in K$ is a matrix it makes sense to multiply $\Phi(x)$ by a $g \times g$ matrix.

Evidently, $\Phi(K)$ is a subring of $\mathbb{C}^g$ isomorphic to K with addition and multiplication coming from matrix addition and matrix multiplication. Furthermore, by Lemma 2.2.3 we have for each $x \in K$

$$\overline{\Phi(x)} = \Phi(\overline{x}).$$

We define an action of K on $M(g, \mathbb{C})$ by letting $\alpha \in K$ act on $X \in M(g, \mathbb{C})$ by

$$\alpha \cdot X = \Phi(\alpha)X. \tag{2.2.7}$$

There are 2^g CM-types of K. Let K_2/K_1 be an extension of CM-fields. Then we can extend any CM-type Φ of K_1 into a CM-type of K_2 by the following process. If $\Phi = \{\phi_1, \ldots, \phi_g\}$, we define the CM-type of K_2 induced by Φ to be the collection

$$\Phi_{K_2} = \{\, \phi \in \mathrm{Hom}(K_1, \mathbb{C}) \mid \phi|_{K_1} \in \Phi \}\,.$$

This is a CM-type by Lemma 2.2.4. We say that a CM-type is primitive if it is not induced from a CM-type on a strictly smaller CM-field. We will also refer to a CM-field K as primitive if every CM type defined on K is primitive. We say that two CM-types Φ and $\widetilde{\Phi}$ are equivalent if there is an automorphism σ of K such that $\Phi = \widetilde{\Phi}\sigma$.

We will in particular focus on the example of a quartic CM-field, so we list the possible CM-types on a quartic CM-field.

Example 2.2.6. Let K be a quartic CM-field. Let $\rho : K \to K$ denote complex conjugation. Then there exist four distinct embeddings of K into $\mathbb{C}$. Let these be $\phi_1, \phi_2, \rho \circ \phi_1, \rho \circ \phi_2$. Let $\Phi = \{\phi_1, \phi_2\}$ and $\widetilde{\Phi} = \{\phi_1, \rho \circ \phi_2\}$. Then exactly one of the following holds.

(1) K contains a quadratic imaginary subfield. Then K is a Galois extension of $\mathbb{Q}$, and its Galois group is isomorphic to the Klein four-group. In this case, each CM-type is induced from a CM-type on a quadratic imaginary field. The two equivalence classes are $\{\Phi, \Phi\rho\}$ and $\left\{\widetilde{\Phi}, \widetilde{\Phi}\rho\right\}$.
(2) K is a cyclic Galois extension. Each CM-type is primitive and they are all equivalent.
(3) K is non-Galois and its Galois closure has Galois group D_4. Each CM-type is primitive. The equivalence classes of CM-types are $\{\Phi, \Phi\rho\}$ and $\left\{\widetilde{\Phi}, \widetilde{\Phi}\rho\right\}$.

For a proof of this, see [**13**], section 8.4, example 2.

Let L be the Galois closure of K and $G = \mathrm{Gal}(L/\mathbb{Q})$. Note that G acts on the CM-types of K in the following way. An automorphism $\sigma \in G$ acts on $\Phi = \{\phi_1, \ldots, \phi_g\}$ by $\sigma \cdot \Phi = \{\sigma \circ \phi_1, \ldots, \sigma \circ \phi_g\}$. Define the half norm $N_\Phi : K \to L$ and half trace $T_\Phi : K \to L$

of an element $x \in K$ associated to the CM-type Φ by the following formulas:

$$N_\Phi(x) = \prod_{\phi \in \Phi} \phi(x),$$
$$T_\Phi(x) = \sum_{\phi \in \Phi} \phi(x).$$

LEMMA 2.2.7. *Let K be a CM-field. Let Φ be a CM-type on K. Let K_1 be the field generated by elements $T_\Phi(x)$ for $x \in K$. Let H be the subgroup of G which fixes Φ, and let $K_2 = L^H$ be the fixed field corresponding to this subgroup. Then $K_1 = K_2$.*

PROOF. To prove that $K_1 \subseteq K_2$ it suffices to show that the generators of K_1 are in K_2. Let $T_\Phi(x)$ be a generator of K_1. Let $\sigma \in H$ be an automorphism of L which fixes Φ. Thus the map $\phi \mapsto \sigma \circ \phi$ on Φ is a bijection. So we have

$$\begin{aligned}\sigma(T_\Phi(x)) &= \sigma\left(\sum_{\phi \in \Phi} \phi(x)\right) \\ &= \sum_{\phi \in \Phi} (\sigma \circ \phi)(x) \\ &= T_\Phi(x).\end{aligned}$$

We now prove that $K_2 \subseteq K_1$. Note that the half trace is a sum of g embeddings of K into L. The linear independence of characters (see [**1**], Chapter 14, Theorem 7) implies that its image generates a $\mathbb{Q}$-vector space of dimension g, so we must have $K_1 = K_2$. □

The field which satisfies one of the two equivalent definitions in the above lemma is called the reflex field of K, denoted K^r. If K is itself Galois, clearly the reflex field is a subfield of K, but if K is non-Galois this need not be true.

We will repeatedly have use of elements $\delta \in K$ which have the property that $\overline{\delta} = -\delta$ and $\operatorname{Re}\Phi(\delta) \in \mathbb{R}^g_{>0}$. We define some notation to describe these elements. Let T be any subset of the complex numbers and S any set of embeddings of K into the complex numbers. Define:

$$K_S(T) = \{\, x \in K \mid \sigma x \in T \text{ for all } \sigma \in S \}\,. \tag{2.2.8}$$

Of particular interest will be the case when $S = \Phi$ is a CM-type and $T = i\mathbb{R}_{>0}$:

$$K_\Phi(i\mathbb{R}_{>0}) = \{\, x \in K \mid \sigma x \in i\mathbb{R}_{>0} \text{ for all } \sigma \in \Phi \} \tag{2.2.9}$$

We also have that the above set is never empty. We care in particular about the case when K is a quartic CM-field so we only prove the lemma in this case here.

LEMMA 2.2.8. *Let K be a quartic CM-field. Let $\Phi = \{\phi_1, \phi_2\}$ be a CM-type on K. Then $K_\Phi(i\mathbb{R}_{>0})$ is nonempty.*

PROOF. First we show that a nonzero purely imaginary element of K exists. That is, there exists $\alpha \in K$ such that $\overline{\alpha} = -\alpha$. Indeed, if β is any element of $K \smallsetminus K_0$ then $\alpha = \beta - \overline{\beta}$ is purely imaginary.

As α is purely imaginary for each $j = 1, 2$ we have $\phi_j(\alpha) = \alpha_j i$ for some $\alpha_j \in \mathbb{R} \smallsetminus \{0\}$. Thus we have the following four possibilities.

$$\alpha_1 > 0 \text{ and } \alpha_2 > 0, \tag{2.2.10}$$

$$\alpha_1 < 0 \text{ and } \alpha_2 < 0, \tag{2.2.11}$$

$$\alpha_1 > 0 \text{ and } \alpha_2 < 0, \tag{2.2.12}$$

$$\alpha_1 < 0 \text{ and } \alpha_2 > 0. \tag{2.2.13}$$

If (2.2.10) holds then $\alpha \in K_\Phi(i\mathbb{R}_{>0})$. If (2.2.11) holds then $-\alpha \in K_\Phi(i\mathbb{R}_{>0})$. If (2.2.13) holds then (2.2.12) holds for $-\alpha$. It thus suffices to show that $K_\Phi(i\mathbb{R}_{>0})$ is nonempty if (2.2.12) holds.

Suppose there exists $\gamma \in K_0$ with $\phi_1(\gamma) > 0$ and $\phi_2(\gamma) < 0$. Then $\gamma\alpha \in K_\Phi(i\mathbb{R}_{>0})$. Thus it suffices to show that there exists $\gamma \in K_0$ with $\phi_1(\gamma) > 0$ and $\phi_2(\gamma) < 0$.

Let n be a squarefree integer such that $K_0 = \mathbb{Q}(\sqrt{n})$. Let $\epsilon = a + b\sqrt{n} \in K_0$ with $a, b \in \mathbb{Q}$. Note that as Φ is a CM-type $\phi_2 \neq \overline{\phi}_1$ and thus if $\sigma_1 = \phi_1|_{K_0}$ and $\sigma_2 = \phi_2|_{K_0}$ we have $\sigma_1 \neq \sigma_2$ so that, after perhaps exchanging σ_1 with σ_2 we have that $\sigma_1 = 1_{K_0}$ and σ_2 is the automorphism of K_0 which maps $\sqrt{m}$ to $-\sqrt{m}$. We have

$$\phi_1(\epsilon) = a + b\sqrt{n} \text{ and}$$
$$\phi_2(\epsilon) = a - b\sqrt{n}.$$

Thus if we let $\gamma = \sqrt{n}$, then $\phi_1(\gamma) > 0$ and $\phi_2(\gamma) < 0$ as required. □

The following Lemma will be useful in our eventual work. If K is a number field let $U(K)$ denote the group of units of $\mathfrak{O}_K$.

LEMMA 2.2.9. *Let K be a quartic CM-field with no roots of unity other than ± 1. Let K_0 be its maximal totally real subfield. Then $U(K) = U(K_0)$.*

PROOF. The field K is totally imaginary and K_0 is totally real, so K_0 has 2 real embeddings into the complex numbers and K has 2 pairs of complex embeddings into the complex numbers. As neither field contains roots of unity other than ± 1, by Dirichlet's Unit Theorem (see [**10**], Theorem 7.4), we can write $U(K) = \{\pm 1\} \times M$ and $U(K_0) = \{\pm 1\} \times N$ where M and N are free abelian groups of rank 1. Let x be a fundamental unit of K and y a fundamental unit of K_0. As $N \subseteq M$ and both are of rank 1, there exists some number k such that $x^k = y$. As y is real, we have $\overline{x}^k = x^k$. Thus $\left(\frac{\overline{x}}{x}\right)^k = 1$,

so $\frac{\overline{x}}{x}$ is a root of unity. Since by assumption the only roots of unity in K are ± 1, we must have $\frac{\overline{x}}{x} = \pm 1$, or equivalently, $\overline{x} = \pm x$. We also know the sign is not -1, as the only purely imaginary units are $\pm i$ which are not in K, so we must have $\overline{x} = x$, so that x is real. □

2.3. Riemann Forms

Let V be a vector space over a field F of characteristic 0. Let $B = \{b_1, \ldots, b_n\}$ be an F-basis of V. The $\mathbb{Z}$-span of B is called a lattice in V. Note that some sources refer to the $\mathbb{Z}$-span of any linearly independent set as a lattice, but we only use the word lattice to refer to the span of full bases. Such lattices are in some other sources called full lattices or complete lattices.

Of particular interest is the case when $F = \mathbb{R}$. If L is a lattice in a real vector space V We will also call L a complex lattice if the vector space V also carries the structure of a complex vector space. Note that in this case necessarily the rank of L is even. If L is a complex lattice in a complex vector space V, we call V/L a complex torus.

Let L be a complex lattice in $\mathbb{C}^g$. Let $E : L \times L \to \mathbb{Z}$ be a $\mathbb{Z}$-bilinear form. Denote by $E_{\mathbb{R}}$ the $\mathbb{R}$-bilinear form $\mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ obtained by linearly extending the form on L. More precisely, as L is a lattice in $\mathbb{C}^g$, it contains an $\mathbb{R}$-basis of $\mathbb{C}^g$ so there is a unique $\mathbb{R}$-bilinear function $E_{\mathbb{R}}$ such that $E_{\mathbb{R}}(x, y) = E(x, y)$ for all $x, y \in L$. Assume that E is alternating, that is, that

$$E(x, x) = 0 \text{ for all } x \in L.$$

Because $\mathbb{C}$ has characteristic 0, this is equivalent to E being skew-symmetric, that is

$$E(y, x) = -E(x, y) \text{ for all } x, y \in L.$$

Note that this implies the same properties are true of $E_{\mathbb{R}}$. Let H denote the function $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ defined by

$$H(x, y) = E_{\mathbb{R}}(ix, y) + iE_{\mathbb{R}}(x, y)$$

for all $x, y \in \mathbb{C}^g$.

Definition 2.3.1. Let $E : L \times L \to \mathbb{Z}$, $E_{\mathbb{R}} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ and $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}^g$ be the functions defined above. We call E a Riemann form if they have the following properties:

(1) $E_{\mathbb{R}}(ix, iy) = E_{\mathbb{R}}(x, y)$ for all $(v, w) \in \mathbb{C}^g \times \mathbb{C}^g$.
(2) The function $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ is a positive definite Hermitian form.

REMARK 2.3.2. The fact that H is a Hermitian form is equivalent to the first condition. Indeed, if $E_{\mathbb{R}}(ix, iy) = E_{\mathbb{R}}(x, y)$ for all $x, y \in \mathbb{C}^g$, we have

$$\begin{aligned} H(y, x) &= E_{\mathbb{R}}(iy, x) + iE_{\mathbb{R}}(y, x) \\ &= -E_{\mathbb{R}}(x, iy) - iE_{\mathbb{R}}(x, y) \\ &= E_{\mathbb{R}}(ix, y) - iE_{\mathbb{R}}(x, y) \\ &= \overline{H(x, y)} \end{aligned}$$

for all $x, y \in \mathbb{C}^g$. Conversely, if H is Hermitian so that $H(y, x) = \overline{H(x, y)}$ for all $x, y \in \mathbb{C}^g$, then in particular we have

$$\begin{aligned} H(x, iy) &= E_{\mathbb{R}}(ix, iy) + iE_{\mathbb{R}}(x, iy), \\ \overline{H(iy, x)} &= E_{\mathbb{R}}(-y, x), -iE_{\mathbb{R}}(iy, x) \end{aligned}$$

so that, by equating real parts,

$$E_{\mathbb{R}}(ix, iy) = E_{\mathbb{R}}(-y, x) = -E_{\mathbb{R}}(y, x) = E_{\mathbb{R}}(x, y).$$

We have used the fact that $E_{\mathbb{R}}$ is an alternating bilinear form.

Also note that the second condition is equivalent to the map $\mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ given for $x, y \in \mathbb{C}^g$ by $E_{\mathbb{R}}(ix, y)$ being positive definite. Indeed, as $E_{\mathbb{R}}$ is alternating, if $x \in \mathbb{C}^g$,

$$H(x, x) = E_{\mathbb{R}}(ix, x) + iE_{\mathbb{R}}(x, x) = E_{\mathbb{R}}(ix, x)$$

so that $H(x, x) = 0$ if and only if $E_{\mathbb{R}}(x, x) = 0$.

EXAMPLE 2.3.3. Consider the lattice $L = \mathbb{Z} + i\mathbb{Z}$ in $\mathbb{C}$. We can define a $\mathbb{Z}$-bilinear form E on L by

$$E(a + bi, c + di) = bc - ad.$$

Then E is an alternating form, and if $z = a + bi, w = c + di \in \mathbb{C}$,

$$\begin{aligned} H(z, w) &= E_{\mathbb{R}}(iz, w) + iE_{\mathbb{R}}(z, w) \\ &= E_{\mathbb{R}}(-b + ai, c + di) + iE_{\mathbb{R}}(a + bi, c + di) \\ &= ac + bd + (bc - ad)i \\ &= z\overline{w}. \end{aligned}$$

In particular, $H(z, z) = |z|^2$ so that H is a positive definite Hermitian form and E is a Riemann form.

To characterize polarizations we need a basis which is described below.

THEOREM 2.3.4. *Let K be a CM-field with a CM-type Φ. Let $\mathfrak{c}$ be a fractional ideal of K and L be the lattice $\Phi(\mathfrak{c}) \subseteq \mathbb{C}^g$. Let E be a Riemann form on L. Then there exists*

elements $y_1, y_2, \ldots, y_g, z_1, z_2, \ldots, z_g$ *in* $\Phi(K)$ *and unique positive integers* $m_1, \ldots, m_g$ *such that* $m_1|m_2, m_2|m_3, \ldots m_{g-1}|m_g$,

$$L = y_1\mathbb{Z} + y_2\mathbb{Z} + \cdots + y_g\mathbb{Z} + m_1z_1\mathbb{Z} + m_2z_2\mathbb{Z} + \cdots + m_gz_g\mathbb{Z},$$

and such that for each pair of indices j, k, $E(y_j, y_k) = E(z_j, z_k) = 0$ *and* $E(y_j, z_k) = \delta_{jk}$.

PROOF. This is a specialization of Proposition 1.3 of [**14**]. Shimura proves a more general result for alternating forms on arbitrary Dedekind domains, but this theorem is a special case which is all that is necessary for our purposes. □

DEFINITION 2.3.5. Let E be a Riemann form defined on a lattice L. The basis given in Theorem 2.3.4 is called a canonical basis for L relative to E. When you have a canonical basis for L relative to Eyou also have the associated tuple $(m_1 \ldots, m_g)$. This is called the type of E.

Let V be a finite-dimensional complex vector space of dimension g and let L be a lattice in V. Let G be the set of all Riemann forms $L \times L \to \mathbb{Z}$. Assume that G is non-empty. The set G is a semi-group under addition. Two elements E_1 and E_2 of G are said to be commensurable if there exist positive integers n_1 and n_2 such that $n_1E_1 = n_2E_2$. Commensurability is an equivalence relation on G. Any equivalence class of G with respect to commensurability is called a polarization of L. Let P be a polarization of L, let $E \in P$ and let $(m_1, \ldots, m_g)$ be the type of E as in Theorem 2.3.4. Then $m_1^{-1}E$ is also contained in P and has type $(1, \frac{m_2}{m_1}, \ldots, \frac{m_g}{m_1})$; we thus may assume that $m_1 = 1$. It is straightforward to verify that every element of P is a positive integer multiple of E and in fact that E is the unique element of P with this property. We refer to this unique element E of P as the minimal element of P. If E is the minimal element of P, then we refer to the type of E as the type of the polarization P. If the type of P is $(1, \ldots, 1)$, then we say that P is a principal polarization.

2.4. Bilinear Forms on CM-Fields

The purpose of this section is to establish the properties of certain lattices contained in CM-fields. Our first proposition introduces these lattices and proves that they are in fact lattices.

PROPOSITION 2.4.1. *Let* K *be a CM-field,* Φ *a CM-type on* K *and* $\mathfrak{c}$ *a fractional ideal of* K. *Let* $L = \Phi(\mathfrak{c})$. *Then* L *is a lattice in* $\mathbb{C}^g$.

PROOF. Let $a_1, \ldots, a_{2g}$ be a basis of $\mathfrak{c}$ over $\mathbb{Z}$. Then because this is a basis, the discriminant of this basis is nonzero. The discriminant is the determinant of the matrix

$$\begin{pmatrix} \phi_1(a_1) & \phi_2(a_1) & \ldots & \phi_g(a_1) & \phi_1(\overline{a_1}) & \ldots & \phi_g(\overline{a_1}) \\ \phi_1(a_2) & \phi_2(a_2) & \ldots & \phi_g(a_2) & \phi_1(\overline{a_2}) & \ldots & \phi_g(\overline{a_2}) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \phi_1(a_{2g}) & \phi_2(a_{2g}) & \ldots & \phi_g(a_{2g}) & \phi_1(\overline{a_{2g}}) & \ldots & \phi_g(\overline{a_{2g}}) \end{pmatrix}.$$

Because $\Phi|_{\mathfrak{c}} : \mathfrak{c} \to \Phi(\mathfrak{c})$ defines a bijective $\mathbb{Z}$-linear map, $\Phi(a_1), \ldots, \Phi(a_{2g})$ defines a $\mathbb{Z}$-basis of L. Note that, if we denote the elements of this basis by $v_1, \ldots, v_{2g}$ respectively, the matrix above has the form

$$\begin{pmatrix} v_1 & \overline{v}_1 \\ v_2 & \overline{v}_2 \\ \vdots & \vdots \\ v_{2g} & \overline{v}_{2g} \end{pmatrix}$$

Thus, this $\mathbb{Z}$-basis is linearly independent over $\mathbb{R}$ if and only if the above matrix has nonzero determinant, which was already noted to be true. Therefore L is a lattice in $\mathbb{C}^g$. □

The reason we care about these lattices in particular is they admit an action of $\mathfrak{O}_K$. This property will eventually supply important connections to algebraic geometry. We will discuss this later, however.

Our eventual goal is to discuss the necessary and sufficient conditions for these lattices to admit Riemann forms. To this end we will need a a few results on a certain class of bilinear forms described as follows:

DEFINITION 2.4.2. Let K be a CM-field of degree $2g$ and $\mathfrak{c}$ a fractional ideal of K. Let Φ be a CM-type on K. Let $L = \Phi(\mathfrak{c}) \subset \mathbb{C}^g$. Let $B : L \times L \to \mathbb{Z}$ be a $\mathbb{Z}$-bilinear form on L. We say that B is compatible with complex multiplication if for every $a \in \mathfrak{O}_K$ and $u, v \in \Phi(\mathfrak{c})$, we have

$$B(au, v) = B(u, \overline{a}v).$$

Note that in the case that $E : L \times L$ is compatible with complex multiplication, then the $\mathbb{R}$-linear extension $E_{\mathbb{R}} : \mathbb{C}^g \times \mathbb{C}^g$ satisfies the same identity when $a \in \mathbb{C}$ and $u, v \in \mathbb{C}^g$. In addition, the form $E_K : K \times K \to \mathbb{Q}$ defined by pulling back E to $\mathfrak{c} \times \mathfrak{c}$ and extending $\mathbb{Q}$-linearly to $K \times K$ satisfies the same equality when $a, u, v \in K$. Because of this we will also refer also to $\mathbb{Q}$-bilinear forms on K and $\mathbb{C}^g$ satisfying these equalities as compatible with complex multiplication.

LEMMA 2.4.3. *Let K be a CM-field, Φ a primitive CM-type on K and $\mathfrak{c}$ a fractional ideal of K. Let $L = \Phi(\mathfrak{c})$. If $E : L \times L \to \mathbb{Z}$ is any Riemann form, then E is compatible with complex multiplication.*

PROOF. This is proven in [**13**], though not in exactly this form. This is a result of equation (3) in Theorem 4 of Section 6.2. □

LEMMA 2.4.4. *Let K be a CM-field. Let $\mathfrak{c}$ be a fractional ideal of K, Φ a primitive CM-type on K. Let $L = \Phi(\mathfrak{c})$. Let $B : L \times L \to \mathbb{Z}$ be a nondegenerate $\mathbb{Z}$-bilinear form which is compatible with complex multiplication. Let $B_{\mathfrak{c}} : \mathfrak{c} \times \mathfrak{c} \to \mathbb{Z}$ be the $\mathbb{Z}$-bilinear form on $\mathfrak{c}$ defined so that $B_{\mathfrak{c}}(x, y)$ is equal to $B(\Phi(x), \Phi(y))$ for all $x, y \in \mathfrak{c}$, and let $B_K : K \times K \to \mathbb{Q}$ be the unique $\mathbb{Q}$-bilinear form which extends $B_{\mathfrak{c}}$ to $K \times K$. Then there exists an element $\xi \in K$ such that for all $x, y \in K$ we have*

$$B_K(x, y) = Tr_{\mathbb{Q}}^K(\xi \overline{x} y).$$

PROOF. For each $\xi \in K$ define a function $T_\xi : K \to \mathbb{Q}$ which for $x \in K$ is defined by $T_\xi(x) = \mathrm{Tr}_{\mathbb{Q}}^K(\xi x)$. Note that the trace form which maps $(x, y) \in K \times K$ to $\mathrm{Tr}_{\mathbb{Q}}^K(xy)$ is a nondegenerate bilinear form. Therefore every $\mathbb{Q}$-linear functional $K \to \mathbb{Q}$ is of the form T_ξ for some $\xi \in K$.

Returning to our setting, we use our bilinear form B_K to produce a $\mathbb{Q}$-linear functional $K \to \mathbb{Q}$. For each $x \in K$ let $f_B(x) : K \to \mathbb{Q}$ denote the linear functional defined for all $y \in K$ by$f_B(x)(y) = B_K(x, y)$. The compatibility of $B_{\mathfrak{c}}$ with complex multiplication gives the following equality for every $a, x, y \in K$:

$$f_B(ax)(y) = f_B(x)(\overline{a} y).$$

Note that in particular we have $f_B(x)(y) = f_B(1)(\overline{x} y)$. As $f_B(1)$ is a bilinear form $K \times K \to \mathbb{Q}$ by our earlier discussion there exists $\xi \in K$ such that for all $x \in K$ we have $f_B(1) = \mathrm{Tr}_{\mathbb{Q}}^K(\xi x)$. So if $x, y \in K$ we have that

$$f_B(1)(\overline{x} y) = \mathrm{Tr}_{\mathbb{Q}}^K(\xi \overline{x} y).$$

By the rule coming from complex multiplication, this means that

$$f_B(x)(y) = \mathrm{Tr}_{\mathbb{Q}}^K(\xi \overline{x} y)$$

for $x, y \in K$. This by definition means that

$$B_K(x, y) = \mathrm{Tr}_{\mathbb{Q}}^K(\xi \overline{x} y)$$

for $x, y \in K$. □

We are now prepared to prove the following result.

PROPOSITION 2.4.5. *Let K be a CM-field. Let $\mathfrak{c}$ be a fractional ideal of K, Φ a primitive CM-type on K. Let $L = \Phi(\mathfrak{c})$. Let $E : L \times L \to \mathbb{Z}$ be a Riemann form on L. Then there exists a $\delta \in K$ with the property that δ^{-1} is in $K_\Phi(i\mathbb{R}_{>0})$ and for all $x, y \in \mathfrak{c}$ we have*

$$E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1}\overline{x}y).$$

PROOF. Note that by Lemma 2.4.3 the Riemann form E is compatible with complex multiplication. So Lemma 2.4.4 implies that there exists $\xi \in K$ such that for $x, y \in K$, $E_K(x, y) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi\overline{x}y)$. Let $\delta = \xi^{-1}$. It only remains to prove that δ has the desired characteristics. Let E_{K_0} denote the restriction of E_K to K_0. First we show that E_{K_0} is a symmetric form. Note that $\mathfrak{O}_{K_0}$ contains a basis of K_0, so it suffices to show this for $x, y \in \mathfrak{O}_{K_0}$. As K_0 is totally real, for $x, y \in \mathfrak{O}_{K_0}$, $\overline{x} = x$ and $\overline{y} = y$. We have that for all $x, y \in \mathfrak{O}_{K_0}$,

$$\begin{aligned} E_{K_0}(x, y) &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi\overline{x}y) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi xy) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi\overline{y}x) \\ &= E_{K_0}(y, x). \end{aligned}$$

Thus E_{K_0} is a symmetric form. But we also have that E_{K_0} is alternating, so for $x, y \in K_0$,

$$\begin{aligned} 0 &= E_{K_0}(x + y, x + y) \\ &= E_{K_0}(x, x) + E_{K_0}(y, y) + 2E_{K_0}(x, y) \\ &= 2E_{K_0}(x, y). \end{aligned}$$

Therefore, E_K restricts to the zero form on K_0. More explicitly, this means that for all $x, y \in K_0$, we have

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi xy) &= 0 \\ \mathrm{Tr}_{\mathbb{Q}}^{K_0}(\mathrm{Tr}_{K_0}^{K}(\xi xy)) &= 0 \\ Tr_{\mathbb{Q}}^{K_0}((\xi + \overline{\xi})xy) &= 0. \end{aligned}$$

This is in particular true when $x = 1$ which implies, because the trace form is nondegenerate, that $\xi + \overline{\xi} = 0$. So ξ is imaginary and therefore δ is also imaginary. Now, because δ is imaginary, we can write, for each j, $\phi_j(\delta) = i\delta_j$ for a real number δ_j. We must prove that the δ_j are positive. For this purpose we write a formula for $E_{\mathbb{R}}$. Let $\alpha_1, \ldots, \alpha_{2g}$ be a $\mathbb{Z}$-basis of $\mathfrak{c}$ so that $\Phi(\alpha_1), \ldots, \Phi(\alpha_{2g})$ is a $\mathbb{Z}$-basis of $\Phi(\mathfrak{c})$. For any $r, s \in \{1, \ldots, 2g\}$ we have

$$E(\Phi(\alpha_r), \Phi(\alpha_s)) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi\overline{\alpha}_r\alpha_s)$$

$$= \sum_{t=1}^{g} \phi_t(\xi\overline{\alpha}_r\alpha_s) + \overline{\phi_t(\xi\overline{\alpha}_r\alpha_s)}$$

$$= \sum_{t=1}^{g} \delta_t^{-1}\overline{\phi_t(\alpha_s)}\phi_t(\alpha_r)i - \delta_t^{-1}\overline{\phi_t(\alpha_r)}\phi_t(\alpha_s)i. \tag{2.4.1}$$

Now, for $z = (z_1, \ldots, z_g), w = (w_1, \ldots, w_g) \in \mathbb{C}^g$ the following define $\mathbb{R}$-blinear forms on $\mathbb{C}^g$:

$$E_{\mathbb{R}}(z, w), \qquad \sum_{t=1}^{g} -\delta_t^{-1}(\overline{z_t}w_t i - \overline{w_t}z_t i).$$

Since by (2.4.1) these two $\mathbb{R}$-bilinear forms agree on a basis of $\mathbb{C}^g$ as a real vector space we conclude that they are equal. That is, for $z, w \in \mathbb{C}^g$ we have

$$E_{\mathbb{R}}(z, w) = \sum_{t=1}^{g} -\delta_t^{-1}(\overline{z_t}w_t i - \overline{w_t}z_t i). \tag{2.4.2}$$

Because E is a Riemann form, $E_{\mathbb{R}}$ is the imaginary part of a positive definite Hermitian form H and we have for $x, y \in \mathbb{C}^g$,

$$H(x, y) = E_{\mathbb{R}}(ix, y) + iE_{\mathbb{R}}(x, y).$$

Consider the values of H at vectors e_j which are 1 in the jth position but 0 elsewhere. We have that

$$\begin{aligned} H(e_j, e_j) &= E_{\mathbb{R}}((0, \ldots, i, \ldots, 0), (0, \ldots, 1, \ldots, 0)) \\ &= -\delta_j^{-1}(-i \cdot i - i \cdot i) \\ &= -2\delta_j^{-1} \end{aligned}$$

which implies that the δ_j are all negative. □

We now prove that every element δ such that δ^{-1} is in $K_\Phi(i\mathbb{R}_{>0})$ defines a Riemann form in this way.

Proposition 2.4.6. *Let K be a CM-field with a primitive CM-type Φ. Let $\mathfrak{c}$ be a fractional ideal of K and let $L = \Phi(\mathfrak{c})$. Let D be the different of K. Assume that there exists an element δ in $\mathfrak{c}\overline{\mathfrak{c}}D$ which is such that δ^{-1} is in $K_\Phi(i\mathbb{R}_{>0})$. Then the bilinear form $B : L \times L \to \mathbb{Z}$ defined for all $x, y \in \mathfrak{c}$ by*

$$B(\Phi(x), \Phi(y)) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1}\overline{x}y)$$

is a Riemann form.

Proof. First, note that the form described takes values in the integers. Indeed, as $\mathfrak{c}^{-1}\overline{\mathfrak{c}}^{-1}D^{-1}$ is the trace dual of $\mathfrak{c}\overline{\mathfrak{c}}$ and $\delta^1 \in \mathfrak{c}^{-1}\overline{\mathfrak{c}}^{-1}D^{-1}$, if $x, y \in \mathfrak{c}$, then $\mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1}\overline{x}y)$ is in

$\mathbb{Z}$. We prove that B is an alternating form. Let $x \in \mathfrak{c}$. Then

$$\begin{aligned} B(\Phi(x), \Phi(x)) &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1} x\overline{x}) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(\mathrm{Tr}_{K_0}^{K}(\delta^{-1} x\overline{x})) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(\delta^{-1} x\overline{x} + \overline{\delta^{-1} x\overline{x}}) \\ &= 0. \end{aligned}$$

The last line is justified by the fact that $\delta^{-1} x\overline{x} \in K_\Phi(i\mathbb{R})$. To complete the proof we prove that B is a Riemann form. Let $B_{\mathbb{R}} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ be the real-linear extension of B from L to $\mathbb{C}^g$. Let $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ be the bilinear form given for $z, w \in \mathbb{C}^g$ by

$$H(z, w) = B_{\mathbb{R}}(iz, w) + iB_{\mathbb{R}}(z, w).$$

We first prove (1) of 2.3.1. For this, we calculate a formula for $B_{\mathbb{R}}$. Let $a_1, \ldots, a_{2g}$ be a $\mathbb{Z}$-basis of $\mathfrak{c}$ so that $\Phi(a_1), \ldots \Phi(a_{2g})$ is a basis of L. Because L spans $\mathbb{C}^g$ as an $\mathbb{R}$-vector space, this is also an $\mathbb{R}$-basis of $\mathbb{C}^g$. Let $\Phi = \{\phi_1, \ldots, \phi_g\}$. For each j, let $\delta_j = \mathrm{Im}(\phi_j(\delta))$. Then for $k, l \in \{1, \ldots, g\}$,

$$\begin{aligned} B_{\mathbb{R}}(\Phi(a_k), \Phi(a_l)) &= B(\Phi(a_k), \Phi(a_l)) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1}\overline{a}_k a_l) \\ &= \sum_{r=1}^{g} \phi_r(\delta^{-1}\overline{a}_k a_l) + \overline{\phi_r(\delta^{-1}\overline{a}_k a_l)} \\ &= \sum_{r=1}^{g} -i\delta_r^{-1}\overline{\phi_r(a_k)}\phi_r(a_l) + i\delta_r^{-1}\phi_r(a_k)\overline{\phi_r(a_l)}. \end{aligned}$$

Because this formula holds on a basis of $\mathbb{C}^g$ we conclude that the form $B_{\mathbb{R}}$ is given for $z = (z_1, \ldots, z_g)$ and $w = (w_1, \ldots, w_g)$ by the formula

$$B_{\mathbb{R}}(z, w) = \sum_{r=1}^{g} -i\delta_r^{-1}(\overline{z}_r w_r - z_r\overline{w}_r).$$

This is by the same reasoning as the derivation done in Proposition 2.4.5. We now calculate for $z = (z_1, \ldots, z_g)$ and $w = (w_1, \ldots w_g) \in \mathbb{C}^g$

$$\begin{aligned} B_{\mathbb{R}}(iz, iw) &= \sum_{r=1}^{g} -i\delta_r^{-1}(\overline{iz_r} iw_r - iz_r\overline{iw_r}) \\ &= \sum_{r=1}^{g} -i\delta_r^{-1}(\overline{z}_r w_r - z_r\overline{w}_r) \\ &= B_{\mathbb{R}}(z, w). \end{aligned}$$

We now show (2) of Definition 2.3.1. Because B is alternating, it suffices to show that $\mathrm{Re}(H)$ is positive definite. We have

$$\begin{aligned} B_{\mathbb{R}}(iz, z) &= \sum_{r=1}^{g} -i\delta_r^{-1}(\overline{iz_r}z_r - iz_r\overline{z}_r) \\ &= \sum_{r=1}^{g} -2\delta_r^{-1}z_r\overline{z}_r \end{aligned}$$

which is positive because δ_r is negative for each r. This completes the proof. □

We have now proven that Riemann forms E on L are fully characterized by a choice of element δ such that δ^{-1} is in $\mathfrak{c}^{-1}\overline{\mathfrak{c}}^{-1}D^{-1}$, and δ^{-1} is in $K_\Phi(i\mathbb{R}_{>0})$. We can actually say more about δ depending on what the type of E is.

Definition 2.4.7. Let Λ be a lattice in a vector space V over a field F and $B : V \times V \to F$ be a nondegenerate F-bilinear form on V which restricts to a $\mathbb{Z}$-bilinear form on Λ. The dual of Λ with respect to B, denoted $\Lambda^\sharp$, is

$$\Lambda^\sharp = \{\, x \in V \mid B(x, \Lambda) \subseteq \mathbb{Z} \,\}. \tag{2.4.3}$$

We say that Λ is self-dual with respect to B if $\Lambda = \Lambda^\sharp$.

We have the following result.

Lemma 2.4.8. *Let K be a CM-field and Φ a CM-type on K. Let $\mathfrak{c}$ be a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let E be a Riemann form on L inducing a polarization of type $(m_1, \ldots, m_g)$ and $y_1, \ldots, y_g, m_1z_1, \ldots, m_gz_g$ a canonical basis of L with respect to this Riemann form. Regard L as a lattice inside the $\mathbb{Q}$-vector space $\Phi(K)$. Then we have*

$$L^\sharp = \frac{y_1}{m_1}\mathbb{Z} + \frac{y_2}{m_2}\mathbb{Z} + \cdots + \frac{y_g}{m_g}\mathbb{Z} + z_1\mathbb{Z} + z_2\mathbb{Z} + \cdots + z_g\mathbb{Z}.$$

Proof. This is a routine calculation. □

Lemma 2.4.9. *Let K be a CM-field and Φ a CM-type on K. Let $\mathfrak{c}$ be a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let E be a Riemann form on L. Then E defines a principal polarization if and only if L is self-dual with respect to E.*

Proof. Based on the characterization of $L^\sharp$ from Lemma 2.4.8, $L^\sharp = L$ if and only if $m_1 = m_2 = \cdots = m_g = 1$. □

Lemma 2.4.10. *Let K be a CM-field and Φ a CM-type on K. Let $\mathfrak{c}$ be a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let E be a Riemann form on L of type $(m_1, \ldots, m_g)$ and*

$y_1, \ldots, y_g, m_1 z_1, \ldots, m_g z_g$ a canonical basis of L with respect to this Riemann form. Regard L as a lattice inside the $\mathbb{Q}$-vector space $\Phi(K)$. Then we have the following isomorphism of abelian groups.

$$L^\sharp / L \simeq (\mathbb{Z}/m_1\mathbb{Z})^2 \times (\mathbb{Z}/m_2\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/m_g\mathbb{Z})^2 .$$

PROOF. We have

$$\begin{aligned} L^\sharp/L &= \frac{\frac{y_1}{m_1}\mathbb{Z} + \frac{y_2}{m_2}\mathbb{Z} + \cdots + \frac{y_g}{m_g}\mathbb{Z} + z_1\mathbb{Z} + z_2\mathbb{Z} + \cdots + z_g\mathbb{Z}}{y_1\mathbb{Z} + y_2\mathbb{Z} + \cdots + y_g\mathbb{Z} + m_1 z_1\mathbb{Z} + m_2 z_2\mathbb{Z} + \cdots + m_g z_g\mathbb{Z}} \\ &\simeq \frac{\frac{y_1}{m_1}\mathbb{Z}}{y_1\mathbb{Z}} \times \frac{\frac{y_2}{m_2}\mathbb{Z}}{y_2\mathbb{Z}} \times \cdots \times \frac{\frac{y_g\mathbb{Z}}{m_g\mathbb{Z}}}{y_g\mathbb{Z}} \times \frac{z_1\mathbb{Z}}{m_1 z_1\mathbb{Z}} \times \frac{z_2\mathbb{Z}}{m_2 z_2\mathbb{Z}} \times \cdots \times \frac{z_g\mathbb{Z}}{m_g z_g\mathbb{Z}} \\ &\simeq (\mathbb{Z}/m_1\mathbb{Z})^2 \times (\mathbb{Z}/m_2\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/m_g\mathbb{Z})^2 . \end{aligned}$$

This proves the result. □

We need another lemma to build toward our main result.

LEMMA 2.4.11. *Let K be a CM-field with primitive CM-type Φ and different D. Let $\mathfrak{c}$ be a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let E be a Riemann form on L. By Proposition 2.4.5 there exists $\delta \in K$ which is such that δ^{-1} is in $K_\Phi(i\mathbb{R}_{>0})$ such that E is given by the formula*

$$E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{\mathbb{Q}}^K(\delta^{-1}\overline{x}y)$$

for all $\Phi(x), \Phi(y) \in L$. We then have

$$L^\sharp = \Phi(\delta\overline{\mathfrak{c}}^{-1}D^{-1}).$$

PROOF. For a lattice $\Lambda \subseteq K$, let $\Lambda^\vee$ denote the trace dual of Λ in K. Note that for fractional ideals $\mathfrak{r}$ we have $\mathfrak{r}^\vee = \mathfrak{r}^{-1}D^{-1}$. In particular, $D^{-1} = \mathfrak{O}_K^\vee$. We have

$$\begin{aligned} L^\sharp = \Phi(\mathfrak{c})^\sharp &= \{\, w \in \Phi(K) \mid E_K(w, \Phi(\mathfrak{c})) \subseteq \mathbb{Z}\} \\ &= \left\{ w \in \Phi(K) \mid \mathrm{Tr}_{\mathbb{Q}}^K(\delta^{-1}\overline{\Phi^{-1}(w)}\mathfrak{c}) \subseteq \mathbb{Z} \right\} \\ &= \Phi\left(\left\{ x \in K \mid \mathrm{Tr}_{\mathbb{Q}}^K(\delta^{-1}\overline{x}\mathfrak{c}) \subseteq \mathbb{Z} \right\}\right) \\ &= \Phi\left(\left\{ x \in K \mid \mathrm{Tr}_{\mathbb{Q}}^K(\delta^{-1}x\overline{\mathfrak{c}}) \subseteq \mathbb{Z} \right\}\right) \\ &= \Phi\left(\left(\delta^{-1}\overline{\mathfrak{c}}\right)^\vee\right) \\ &= \Phi\left(\delta\overline{\mathfrak{c}}^{-1}D^{-1}\right). \end{aligned}$$

This completes the proof. □

2.5. Abelian Varieties

An abelian variety over a field K is a group variety over K that is, as a variety, connected and complete. In particular, an abelian variety has a group structure which is abelian. For example, an elliptic curve is an abelian variety of dimension one. Abelian varieties over the complex numbers have a very rigid structure.

THEOREM 2.5.1. *If A is an abelian variety of dimension g defined over the complex numbers then there exists a lattice L in $\mathbb{C}^g$ such that $A(\mathbb{C}) \simeq \mathbb{C}^g/L$ and there exists a Riemann form $L \times L \to \mathbb{Z}$. Conversely, if L is a lattice in $\mathbb{C}^g$ for some positive integer g and there exists a Riemann form $L \times L \to \mathbb{Z}$ then $\mathbb{C}^g/L$ is an abelian variety.*

PROOF. The proof is long. An outline is given in Chapter 3 of [**13**], although he neglects to prove some details. In particular, Shimura neglects to prove that his construction of a Riemann form from a holomorphic theta function works. To see details on these, see [**3**], Chapter 4 or [**5**], Chapter 5. □

Let A be an abelian variety of dimension g and let L be a lattice in $\mathbb{C}^g$ such that $A \simeq \mathbb{C}^g/L$. We define a polarization of A to be a polarization P of L, and we refer to the pair (A, P) as a polarized abelian variety.

We list some properties of transformations of abelian varieties which will motivate the primary objects of study for this thesis. We make many claims without proof but proofs can be found in the early chapters of [**13**] or [**6**].

Let A and B be abelian varieties. A homomorphism of abelian varieties from A to B is a map $A \to B$ which is a homomorphism of group varieties. We denote the set of all homomorphisms of abelian varieties from A to B by $\mathrm{Hom}(A, B)$. This is an abelian group under addition. A homomorphism from an abelian variety A to itself is called an endomorphism. We write $\mathrm{End}(A) = \mathrm{Hom}(A, A)$. This is a ring with addition and composition of functions as its operations. An isogeny from A to B is a surjective homomorphism of abelian varieties with a finite kernel. An abelian variety is called simple if it is not isogenous to a product of lower-dimensional abelian varieties.

Assume that A is an abelian variety over $\mathbb{C}$ of dimension g. Then A is isomorphic to $\mathbb{C}^g/L$ for an appropriate lattice L. In this case, because a homomorphism of group varieties is in particular a homomorphism of complex manifolds. Such a homomorphism lifts from $\mathbb{C}^g/L$ to a linear map $\mathbb{C}^g \to \mathbb{C}^g$. It follows that there is an isomorphism between the ring of endomorphisms $A \to A$ and the ring of linear endomorphisms $\mathbb{C}^g \to \mathbb{C}^g$ which leave L invariant. That is,

$$\mathrm{End}(A) \simeq \{\, \alpha \in \mathrm{M}_g(\mathbb{C}) \mid \alpha L \subseteq L \,\}.$$

Then $\mathrm{End}(A)$ is a finite rank $\mathbb{Z}$-module in $\mathrm{M}_g(\mathbb{C})$ of rank no greater than $2g$. Most abelian varieties will have endomorphism rings of rank less than $2g$. Assume that A is simple and has endomorphism ring of rank $2g$. Then it can be shown that $K = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM-field. Then $\mathrm{End}(A)$ is isomorphic to an order $\mathfrak{O}$ contained in $\mathfrak{O}_K$. In this case, we say that A has complex multiplication by $\mathfrak{O}$.

PROPOSITION 2.5.2. *Let K be a CM-field, $\mathfrak{c}$ a fractional ideal of $\mathfrak{O}_K$ and $L = \Phi(\mathfrak{c})$. Suppose that L admits a Riemann form so that $\mathbb{C}^g/L$ is a polarized abelian variety. Then $\mathbb{C}^g/L$ has complex multiplication by $\mathfrak{O}_K$.*

PROOF. We define an action of $\mathfrak{O}_K$ on $\mathbb{C}^g$ by letting $\alpha \in \mathfrak{O}_K$ act on $z \in \mathbb{C}^g$ by

$$\alpha \cdot z = \Phi(\alpha) z$$

as in Definition 2.2.5. Now, note that as $\mathfrak{c}$ is a fractional ideal of K it has the property that $\alpha\mathfrak{c} \subseteq \mathfrak{c}$, which implies that $\alpha \cdot L \subseteq L$. Therefore the action of $\mathfrak{O}_K$ on $\mathbb{C}^g$ descends to an action of $\mathfrak{O}_K$ on L. So L has complex multiplication by $\mathfrak{O}_K$ □

It is also true that any abelian variety A with complex multiplication by $\mathfrak{O}_K$ is isomorphic to $\mathbb{C}^g/\Phi(\mathfrak{c})$ for some fractional ideal $\mathfrak{c}$ of K.

Chapter 3: Main Results

In this chapter we state and prove the main results of this thesis. The first main result is Theorem 3.1.2 which characterizes exactly when there exists an abelian surface with complex multiplication by the maximal order $\mathfrak{O}_K$ in a given CM-field K admitting a polarization of type $(1, m)$. Such a surface is isomorphic to $\mathbb{C}^2/\Phi(\mathfrak{c})$ where Φ is a primitive CM-type of K and $\mathfrak{c}$ is a fractional ideal of K, such that $\mathfrak{c}\bar{\mathfrak{c}}\,\mathrm{Diff}_{K/\mathbb{Q}} = \delta\mathfrak{a}^{-1}$ for $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$ and $\mathfrak{a}$ a fractional ideal of certain specified forms. This expands upon work by Shimura and Taniyama when $m = 1$.

The remainder of the section deals with corollaries of this result. We derive many necessary conditions for there to be polarized abelian surfaces with complex multiplication by a given CM-field K. Many of these necessary conditions are specific to the case when K is a cyclic Galois extension or to the case when K is a non-Galois extension. These necessary conditions are not sufficient conditions, but if m is a positive integer, whenever there exists a fractional ideal $\mathfrak{a} = \prod_{p|m} \mathfrak{a}_p$ as given in Theorem 3.1.2 and $\mathfrak{a}$ is an extension of an ideal of K_0, we prove in Theorem 3.2.1 that there exists some abelian surface with complex multiplication by K which admits a polarization of type $(1, m)$.

3.1. The Main Theorem

This section is devoted to the proof of the most important theorem in this thesis. We wish to generalize classical results producing elliptic curves with complex multiplication. These classical results are, for instance, the key to many theorems on the generation of class fields of quadratic imaginary fields by values of modular functions at CM-points. Recall that when E is an elliptic curve defined over $\mathbb{C}$ the ring $\mathrm{End}(E)$ is either isomorphic to the integers or to an order $\mathfrak{O}$ in a quadratic imaginary number field K. The theory has been extended by Shimura and Taniyama [**13**] to abelian varieties of higher dimension.

The elliptic curves which have complex multiplication by $\mathfrak{O}$ are those which are isomorphic to $\mathbb{C}/\mathfrak{c}$ where $\mathfrak{c}$ is a fractional ideal of $\mathfrak{O}_K$. Because homothetic lattices produce isomorphic elliptic curves, the isomorphism classes of elliptic curves with complex multiplication correspond to the ideal classes of $\mathfrak{O}_K$. When generalizing this to a field of higher degree, things are more complicated. It is still true that an abelian variety of dimension g is isomorphic as a complex Lie group to a dimension g complex torus, which is a quotient of $\mathbb{C}^g$ by a full rank lattice, but we now have to establish when it is possible to define a polarization on the lattices involved. The aim of this section is to explain how to produce abelian surfaces which have complex multiplication by a specified order $\mathfrak{O}$ in a quartic CM-field K and which have a polarization of a specified type (m_1, m_2).

Notation and conventions. In the remainder of this section unless it is specified otherwise, K will refer to a CM-field with $[K:\mathbb{Q}] = 2g$. Its maximal totally real subfield will be denoted by K_0. We regard K as embedded into the complex numbers so that the map $\rho : \mathbb{C} \to \mathbb{C}$ mapping an element x to its complex conjugate $\overline{x}$ restricts to an embedding of K into $\mathbb{C}$. Let $\mathfrak{O} = \mathfrak{O}_K$ be the ring of integers of K.

Characterization of polarizations. We begin by stating a result already known in the literature (for example in [**13**]) classifying abelian surfaces with complex multiplication which have a principal polarization.

THEOREM 3.1.1. *Let K be a quartic CM-field. Let Φ be a primitive CM-type on K. Let $\mathfrak{O}_K$ be the ring of integers of K and $\mathfrak{c}$ be a fractional ideal of $\mathfrak{O}_K$. Let $L = \Phi(\mathfrak{c})$. There exists a Riemann form E on L which induces a principal polarization on $\mathbb{C}^2/L$ if and only if there exists a number $\delta \in K$ such that $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$ and such that $(\delta) = \mathfrak{c}\overline{\mathfrak{c}}D$. When this is the case, a Riemann form E is defined for all $\Phi(x), \Phi(y) \in L$ by*

$$E(\Phi(x), \Phi(y)) = Tr^K_{\mathbb{Q}}(\delta^{-1}\overline{x}y).$$

The main result of this section is to generalize Theorem 3.1.1 to the case of any polarization. Our theorem can be stated as follows:

THEOREM 3.1.2. *Let K be a quartic CM-field with primitive CM-type Φ, $\mathfrak{c}$ a fractional ideal of K, and $L = \Phi(\mathfrak{c})$. Let m be a positive integer. Let S_m be the set of all ideals $\mathfrak{b}$ which have a factorization of the form*

$$\mathfrak{b} = \mathfrak{c}\overline{\mathfrak{c}}D\prod_{p|m}\mathfrak{a}_p$$

where for each prime $p|m$, $\mathfrak{a}_p$ and $v_p(m)$ satisfy one of the following:

1. *$\mathfrak{a}_p = \mathfrak{p}^{-v_p(m)}$ where $\mathfrak{p}$ is a prime lying over p with $e(\mathfrak{p}|p) = 1, f(\mathfrak{p}|p) = 2$;*
2. *$\mathfrak{a}_p = \mathfrak{p}^{-2v_p(m)}$ where $\mathfrak{p}$ is a prime lying over p with $e(\mathfrak{p}|p) = 2, f(\mathfrak{p}|p) = 1$;*
3. *$\mathfrak{a}_p = \mathfrak{p}_1^{-v_p(m)}\mathfrak{p}_2^{-v_p(m)}$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct primes lying over p with $e(\mathfrak{p}_1|p) = e(\mathfrak{p}_2|p) = 1, f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$;*
4. *$\mathfrak{a}_p = \mathfrak{p}^{-2}$ where $v_p(m) = 1$, and $\mathfrak{p}$ is a prime lying over p where $e(\mathfrak{p}|p) = 4$ and $f(\mathfrak{p}|p) = 1$ or $e(\mathfrak{p}|p) = 3$ and $f(\mathfrak{p}|p) = 1$;*
5. *$\mathfrak{a}_p = \mathfrak{p}^{-1}$ where $v_p(m) = 1$, and $\mathfrak{p}$ is a prime lying over p where $e(\mathfrak{p}|p) = 2$ and $f(\mathfrak{p}|p) = 2$;*
6. *$\mathfrak{a}_p = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}$ where $v_p(m) = 1$, and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct primes lying over p where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ satisfy one of the following.*
   (a) *$e(\mathfrak{p}_1|p) = 3$, $e(\mathfrak{p}_2|p) = 1$ and $f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$;*
   (b) *$e(\mathfrak{p}_1|p) = e(\mathfrak{p}_2|p) = 2$ and $f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$;*

(c) $e(\mathfrak{p}_1|p) = 2$, $e(\mathfrak{p}_2|p) = 1$ *and* $f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$.

Then there exists a Riemann form on L which defines a polarization of type $(1, m)$ if and only if there exists an ideal $\mathfrak{b} \in S_m$ which is principal and of the form $\mathfrak{b} = (\delta)$ where $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$. In this case, the Riemann form is given by the formula

$$E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1}\overline{x}y)$$

for $x, y \in \mathfrak{c}$.

Proof. Assume there exists a Riemann form $E : L \times L \to \mathbb{Z}$ of type $(1, m)$. By Proposition 2.4.5 there exists $\delta \in K$ such that $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$ and $E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta^{-1}xy)$ for all $x, y \in \mathfrak{c}$. By Lemma 2.4.10 we have that if $L^\sharp$ is the dual of L with respect to E then, since the type of E is $(1, m)$, we have, as abelian groups,

$$L^\sharp/L \simeq (\mathbb{Z}/m\mathbb{Z})^2 . \tag{3.1.1}$$

On the other hand, we also have by Lemma 2.4.11 that $L^\sharp \simeq \delta\overline{\mathfrak{c}}^{-1}D^{-1}$. Using Lemma 2.1.1 we have that

$$L^\sharp/L \simeq \delta\overline{\mathfrak{c}}^{-1}D^{-1}/\mathfrak{c} \simeq \mathfrak{O}_K/\delta^{-1}\mathfrak{c}\overline{\mathfrak{c}}D. \tag{3.1.2}$$

Thus, by (3.1.1) and (3.1.2) we have

$$\mathfrak{O}_K/\delta^{-1}\mathfrak{c}\overline{\mathfrak{c}}D \simeq (\mathbb{Z}/m\mathbb{Z})^2 . \tag{3.1.3}$$

Let the prime decomposition of $\delta^{-1}\mathfrak{c}\overline{\mathfrak{c}}D$ be

$$\delta^{-1}\mathfrak{c}\overline{\mathfrak{c}}D = \mathfrak{q}_1^{v_1} \dots \mathfrak{q}_t^{v_t}. \tag{3.1.4}$$

Let the prime decomposition of m be

$$m = p_1^{u_1} \dots p_s^{u_s}. \tag{3.1.5}$$

The Chinese remainder theorem gives us the following equalities:

$$\mathfrak{O}_K/\delta^{-1}\mathfrak{c}\overline{\mathfrak{c}}D \simeq \mathfrak{O}_K/\mathfrak{q}_1^{v_1} \times \dots \times \mathfrak{O}_K/\mathfrak{q}_t^{v_t},$$
$$(\mathbb{Z}/m\mathbb{Z})^2 \simeq (\mathbb{Z}/p_1^{u_1}\mathbb{Z})^2 \times \dots (\mathbb{Z}/p_s^{u_s}\mathbb{Z})^2 .$$

These equalities, together with (3.1.3) now give us

$$\mathfrak{O}_K/\mathfrak{q}_1^{v_1} \times \dots \times \mathfrak{O}_K/\mathfrak{q}_t^{v_t} \simeq (\mathbb{Z}/p_1^{u_1}\mathbb{Z})^2 \times \dots (\mathbb{Z}/p_s^{u_s}\mathbb{Z})^2 . \tag{3.1.6}$$

Note that for each $j = 1, \dots, t$ there is a unique rational prime q_j lying under $\mathfrak{q}_j$ and $\mathfrak{O}/\mathfrak{q}_j^{v_j}$ is q_j-primary. Also note that $(\mathbb{Z}/p_j\mathbb{Z})^2$ is p_j-primary. This implies each prime q_j is contained in the set $\{p_1, \dots p_s\}$. That is, for each $j \in \{1, \dots, t\}$ there exists an $l \in \{1, \dots, s\}$ such that $\mathfrak{q}_j | p_l$. Thus, because of the isomorphism (3.1.3), after a possible

reordering of the primes dividing m, we have for each j, if we define $(\delta^{-1}\mathfrak{c}\bar{\mathfrak{c}}D)_{p_j}$ as in Lemma 2.1.6, then

$$\mathfrak{O}_K/(\delta^{-1}\mathfrak{c}\bar{\mathfrak{c}}D)_{p_j} \simeq \left(\mathbb{Z}/p_j^{u_j}\mathbb{Z}\right)^2.$$

To complete the proof of this direction it will suffice to prove that $\delta^{-1}\mathfrak{c}\bar{\mathfrak{c}}D$ has form as in (1), (2), (3), (4), (5) or (6) in the statement of the theorem. This follows from Lemma 2.1.6 and 2.1.7.

To prove the other direction suppose that S_m contains a fractional ideal $\mathfrak{b}$ which is principal and of the form $\mathfrak{b} = (\delta)$ where $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$. By the definition of S_m we may write $\mathfrak{b}$ in the form

$$\mathfrak{b} = (\delta) = \mathfrak{c}\bar{\mathfrak{c}}D\prod_{p|m}\mathfrak{a}_p$$

where for each $p|m$, $\mathfrak{a}_p$ satisfies one of (1), (2), (3), (4), (5) or (6) as in the statement of the theorem. Note that $\delta \in \mathfrak{c}\bar{\mathfrak{c}}D$. By Proposition 2.4.6 we have that if we define $E : L \times L \to \mathbb{Z}$ by the formula

$$E(\Phi(x), \Phi(y)) = \mathrm{Tr}_{\mathbb{Q}}^K(\delta^{-1}\overline{x}y)$$

for $x, y \in \mathfrak{c}$ then E defines a Riemann form on L. We must show that it defines a Riemann form of type $(1, m)$. Let (m_1, m_2) be the type of the polarization defined by E. If $L^\sharp$ denotes the dual of L with respect to E then by Lemma 2.4.11 and Lemma 2.4.10 respectively, we have

$$L^\sharp/L \simeq \mathfrak{O}_K/\delta^{-1}\mathfrak{c}\bar{\mathfrak{c}}D = \mathfrak{O}_K/\prod_{p|m}\mathfrak{a}_p^{-1} \text{ and} \tag{3.1.7}$$

$$L^\sharp/L \simeq (\mathbb{Z}/m_1\mathbb{Z})^2 \times (\mathbb{Z}/m_2\mathbb{Z})^2. \tag{3.1.8}$$

Using that the $\mathfrak{a}_p$ satisfy one of (1), (2), (3), (4), (5), or (6) and Proposition 2.1.2 one may verify that $\mathfrak{O}_K/\prod_{p|m}\mathfrak{a}_p^{-1} \simeq (\mathbb{Z}/m\mathbb{Z})^2$. This implies that $m_1 = 1$ and $m_2 = m$ by the uniqueness of the canonical decomposition of finite abelian groups. (See [**11**] Corollary 6.11.) □

The following easy result from Theorem 3.1.2 will be necessary in later deriving necessary conditions for the existence of polarizations.

LEMMA 3.1.3. *Let the assumptions and notations be as in Theorem 3.1.2. Assume that there exists a Riemann form on L which defines a polarization of type $(1, m)$. Then for each prime p dividing m the norm of $\mathfrak{a}_p$ is of the form*

$$N(\mathfrak{a}_p) = p^{-2l}$$

for a positive integer l.

PROOF. Let p be a prime dividing m. Because $\mathfrak{a} \in R_m(K)$we must have that $\mathfrak{a}_p$ satisfies one of (1), (2), (3), (4), (5) or (6) of Theorem 3.1.2. We consider each of these in turn.

If $\mathfrak{a}_p$ satisfies (1) then there exists a prime $\mathfrak{p}$ of K over p such that $\mathfrak{a}_p = \mathfrak{p}^{-v_p(m)}$ and $f(\mathfrak{p}|p) = 2$. Thus $N_{\mathbb{Q}}^K(\mathfrak{a}_p) = p^{-2v_p(m)}$. If $\mathfrak{a}_p$ satisfies (2) then there exists a prime $\mathfrak{p}$ of K over p such that $\mathfrak{a}_p = \mathfrak{p}^{-2v_p(m)}$ and $f(\mathfrak{p}|p) = 1$. Thus $N_{\mathbb{Q}}^K(\mathfrak{a}_p) = p^{-2v_p(m)}$. If $\mathfrak{a}_p$ satisfies (3) then there exist primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K over p such that $\mathfrak{a}_p = \mathfrak{p}_1^{-v_p(m)}\mathfrak{p}_2^{-v_p(m)}$ and $f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$. Thus $N_{\mathbb{Q}}^K(\mathfrak{a}_p) = p^{-2v_p(m)}$. If $\mathfrak{a}_p$ satisfies (4) then there exists a prime $\mathfrak{p}$ of K over p such that $\mathfrak{a}_p = \mathfrak{p}^{-2}$ and $f(\mathfrak{p}|p) = 1$. Thus $N_{\mathbb{Q}}^K(\mathfrak{a}_p) = p^{-2}$. If $\mathfrak{a}_p$ satisfies (5) then there exists a prime $\mathfrak{p}$ of K over p such that $\mathfrak{a}_p = \mathfrak{p}^{-1}$ and $f(\mathfrak{p}|p) = 2$. Thus $N_{\mathbb{Q}}^K(\mathfrak{a}_p) = p^{-2}$. If $\mathfrak{a}_p$ satisfies (6) then then there exist primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K over p such that $\mathfrak{a}_p = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}$ and $f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$. Thus $N_{\mathbb{Q}}^K(\mathfrak{a}_p) = p^{-2}$. □

3.2. Corollaries of the Characterization of Polarizations

There are some relatively simple corollaries of Theorem 3.1.2 which we establish in this section. The following new notation will often be useful in the sequel. Let K be a primitive quartic CM-field with CM-type Φ, $\mathfrak{c}$ a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let m be a positive integer. We let $R_m = R_m(K)$ be the set of all fractional ideals $\mathfrak{a} = \prod_{p|m} \mathfrak{a}_p$ where for each $p|m$ we have that $\mathfrak{a}_p$ satisfies one of (1), (2), (3), (4), (5) or (6) in Theorem 3.1.2. We first prove an existence result.

THEOREM 3.2.1. *Let K be a primitive quartic CM-field. Let m be a positive integer. Assume that $\mathfrak{a} = \prod_{p|m} \mathfrak{a}_p$ is a fractional ideal in $R_m(K)$ such that there exists a fractional ideal $\mathfrak{h}$ of K_0 such that $\mathfrak{a} = \mathfrak{h}\mathfrak{O}_K$. Then there exists a fractional ideal $\mathfrak{c}$ and a CM-type Φ such that $\Phi(\mathfrak{c})$ admits a polarization of type $(1, m)$.*

PROOF. This proof uses ideas from Proposition 5.3 in [**17**] and page 41 in [**16**].

Let z be any nonzero element of K such that $\overline{z} = -z$. By [**18**] Theorem 10.1 and the fact that the infinite place of K_0 ramifies in K, we have that the map $N_{K_0}^K : \mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ on class groups induced by the norm map of ideals is surjective. We claim that $z \operatorname{Diff}_{K/\mathbb{Q}} \mathfrak{a}$ is an extension of an ideal $\mathfrak{b}$ in K_0. Indeed, if $\operatorname{Diff}_{K/K_0}$ is the relative different of K over K_0, by Theorem 2.5 in chapter III of [**10**], $\operatorname{Diff}_{K/K_0}$ is generated by elements of the form $f'(\epsilon)$ where $\epsilon \in \mathfrak{O}_K$ is such that $K = K_0(\epsilon)$ and f is the minimal polynomial of ϵ over K_0. As K/K_0 is a quadratic imaginary extension,

$$f(x) = x^2 - (\epsilon + \overline{\epsilon})x + \epsilon\overline{\epsilon},$$

so that

$$f'(\epsilon) = 2\epsilon - \epsilon - \overline{\epsilon} = \epsilon - \overline{\epsilon}.$$

Thus $\operatorname{Diff}_{K/K_0}$ is generated by elements of the form $\epsilon - \overline{\epsilon}$ with $\epsilon \in \mathfrak{O}_K$. For each $\epsilon \in K$, $\epsilon - \overline{\epsilon}$ is purely imaginary in K. So if $\mathfrak{b}_1$ is the ideal in K_0 generated by elements of the form $z^{-1}(\epsilon - \overline{\epsilon})$, then $z^{-1}\operatorname{Diff}_{K/K_0} = \mathfrak{b}_1\mathfrak{O}_K$. And by definition $\operatorname{Diff}_{K_0/\mathbb{Q}}$ is an ideal of K_0. Finally, recall that $\mathfrak{a} = \mathfrak{h}\mathfrak{O}_K$ with $\mathfrak{h}$ a fractional ideal of K_0. Thus

$$\begin{aligned} z^{-1}\operatorname{Diff}_{K/\mathbb{Q}}\mathfrak{a} &= z^{-1}\operatorname{Diff}_{K/K_0}\operatorname{Diff}_{K_0/\mathbb{Q}}\mathfrak{a}\mathfrak{O}_K \qquad \text{(See page 443 in [4])} \\ &= \mathfrak{b}_1\operatorname{Diff}_{K_0/\mathbb{Q}}\mathfrak{h}\mathfrak{O}_K \\ &= \mathfrak{b}\mathfrak{O}_K \end{aligned}$$

where $\mathfrak{b} = \mathfrak{b}_1\mathfrak{h}\operatorname{Diff}_{K_0/\mathbb{Q}}$. Thus by the surjectivity of the norm map on class groups, there exists $y \in K_0^\times$ and a fractional ideal $\mathfrak{c}$ of $\mathfrak{O}_K$ such that

$$\begin{aligned} yN_{K_0}^K(\mathfrak{c}^{-1}) &= \mathfrak{b} \\ yN_{K_0}^K(\mathfrak{c}^{-1})\mathfrak{O}_K &= \mathfrak{b}\mathfrak{O}_K \\ y\mathfrak{c}^{-1}\overline{\mathfrak{c}}^{-1} &= z^{-1}\operatorname{Diff}_{K/\mathbb{Q}}\mathfrak{a} \qquad \text{(see ex. 14, ch. 3 of [7])} \\ yz &= \mathfrak{c}\overline{\mathfrak{c}}\operatorname{Diff}_{K/\mathbb{Q}}\mathfrak{a}. \end{aligned}$$

Note that as $y \in K_0$ and z is purely imaginary, yz is purely imaginary. Thus, by Theorem 3.1.2 there exists a CM type Φ such that $\Phi(\mathfrak{c})$ admits a polarization of type $(1, m)$. □

Using Theorem 3.2.1 we can give a simple sufficient condition for the existence of a $(1, m)$ polarization when m and the discriminant of K are relatively prime.

COROLLARY 3.2.2. *Let K be a primitive quartic CM-field of degree 4 with maximal totally real subfield K_0. Let m be a positive integer. Assume for each prime p dividing m, p is unramified in K and we have*

$$\left(\frac{\operatorname{Disc}_{K_0/\mathbb{Q}}}{p}\right) = 1.$$

Then there exists a fractional ideal $\mathfrak{c}$ of K and a CM-type Φ of K such that $\Phi(\mathfrak{c})$ admits a polarization of type $(1, m)$.

PROOF. By Theorem 3.2.1 it suffices to show that we can find $\mathfrak{a} \in R_m(K)$ such that there exists a fractional ideal $\mathfrak{h}$ of K_0 such that $\mathfrak{a} = \mathfrak{h}\mathfrak{O}_K$. To show this it suffices to show that for each $p|m$ we can find $\mathfrak{a}_p$ such that $\mathfrak{a} = \prod_{p|m}\mathfrak{a}_p$ and there exists a fractional ideal $\mathfrak{h}_p$ of K_0 such that $\mathfrak{a}_p = \mathfrak{h}_p\mathfrak{O}_K$.

Because $\left(\frac{\operatorname{Disc}_{K_0/\mathbb{Q}}}{p}\right) = 1$ we have that p splits in K_0, i.e., there exists a prime $\mathfrak{p}$ of K_0 such that $p\mathfrak{O}_{K_0} = \mathfrak{p}\sigma(\mathfrak{p})$ where σ is the nontrivial automorphism of K_0. If $\mathfrak{p}$ remains inert in K then let $\mathfrak{h}_p = \mathfrak{p}^{-v_p(m)}$ and $\mathfrak{a}_p = \mathfrak{h}_p\mathfrak{O}_K$. Then we have that $\mathfrak{a}_p$ satisfies (1) of Theorem 3.1.2. If $\mathfrak{p}$ splits in K so that $\mathfrak{p}\mathfrak{O}_K = \mathfrak{P}\overline{\mathfrak{P}}$ for a prime $\mathfrak{P}$ of K, let $\mathfrak{h}_p = \mathfrak{p}^{-v_p(m)}$

and $\mathfrak{a}_p = \mathfrak{h}_p\mathfrak{O}_K = \mathfrak{P}^{-v_p(m)}\overline{\mathfrak{P}}^{-v_p(m)}$. Then we have that $\mathfrak{a}_p$ satisfies (3). In either case there exists a fractional ideal $\mathfrak{h}_p$ of K_0 such that $\mathfrak{a}_p = \mathfrak{h}_p\mathfrak{O}_K$ so that there exists some fractional ideal $\mathfrak{c}$ of K and some CM-type Φ such that $\Phi(\mathfrak{c})$ admits a polarization of type $(1, m)$. □

COROLLARY 3.2.3. *Let K be a primitive quartic CM-field with CM-type Φ, $\mathfrak{c}$ a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let p be a rational prime and let m be a positive integer such that $p|m$. Assume that $\mathbb{C}^2/\Phi(\mathfrak{c})$ admits a polarization of type $(1, m)$. Then p is not inert in K.*

PROOF. This follows immediately from Theorem 3.1.2. □

LEMMA 3.2.4. *Let K be a primitive quartic CM-field with CM-type Φ, $\mathfrak{c}$ a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let m be a positive integer. Then each element $\mathfrak{r}$ of R_m which satisfies $\mathfrak{c}\bar{\mathfrak{c}}\,\mathrm{Diff}_{K/\mathbb{Q}}\,\mathfrak{r} = (\delta)$ for some $\delta \in K_\Phi(i\mathbb{R})$ is invariant under complex conjugation.*

PROOF. This follows from the fact that (δ) and $\mathrm{Diff}_{K/\mathbb{Q}}$ are invariant under complex conjugation. □

Corollary 3.2.2 described what happened when a prime was split in the totally real subfield. The following corollary tells us what happens when it is inert in the totally real subfield.

COROLLARY 3.2.5. *Let K be a primitive quartic CM-field with CM-type Φ, $\mathfrak{c}$ a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Let p be a rational prime and let m be a positive integer such that $p|m$. Suppose that p is inert in $\mathfrak{O}_{K_0}$ and that $\mathbb{C}^2/L$ admits a polarization of type $(1, m)$. Then p ramifies in $\mathfrak{O}_K$ and $v_p(m) = 1$.*

PROOF. Suppose that p is inert in $\mathfrak{O}_{K_0}$ and that $\mathbb{C}^2/L$ admits a polarization of type $(1, m)$. We have that $f(\mathfrak{r}|p) \geqslant 2$ for any prime $\mathfrak{r}$ of $\mathfrak{O}_K$ dividing p. Because $\mathbb{C}^2/L$ admits a polarization of type $(1, m)$ by Theorem 3.1.2 there exists $\delta \in K_\Phi(\mathbb{R}_{>0})$ and $\mathfrak{r} \in R_m$ with $(\delta) = \mathfrak{c}\bar{\mathfrak{c}}D\mathfrak{r}$ and $\mathfrak{r} = \prod_{q|m}\mathfrak{a}_q$ and for all $q|m$ $\mathfrak{a}_q$ satisfying one of (1), (2), (3), (4), (5), or (6) of Theorem 3.1.2. This implies that p is not totally inert in $\mathfrak{O}_K$. Let $\mathfrak{q} = p\mathfrak{O}_{K_0}$; by assumption $\mathfrak{q}$ is prime. Either $\mathfrak{q} = \mathfrak{p}_1\mathfrak{p}_2$ for distinct primes $\mathfrak{p}_1, \mathfrak{p}_2$ in $\mathfrak{O}_K$ or p ramifies in $\mathfrak{O}_K$. Suppose the first case is true. Because K is a quadratic imaginary extension of K_0, we must have that $\mathfrak{p}_1 = \overline{\mathfrak{p}}_2$. Because $\mathfrak{a}_p$ satisfies (1), (2), (3), (4), (5) or (6) of Theorem 3.1.2, it follows that that $\mathfrak{a}_p$ satisfies (1) of Theorem 3.1.2. But this is impossible because in case (1), $\mathfrak{a}_p = \mathfrak{p}^{-v_p(m)}$ where either $\mathfrak{p} = \mathfrak{p}_1$ or $\mathfrak{p} = \mathfrak{p}_2$, neither of which make $\mathfrak{a}_p$ invariant under complex conjugation. This contradicts Lemma 3.2.4. It follows that p is ramified in $\mathfrak{O}_K$. Because $\mathfrak{a}_p$ satisfies (1), (2), (3), (4), (5) or (6) of Theorem 3.1.2 and p ramifies in $\mathfrak{O}_K$ and p is inert in $\mathfrak{O}_{K_0}$ we now see that $\mathfrak{a}_p$ must satisfy (5) of Theorem 3.1.2. This implies $v_p(m) = 1$. □

3.3. Necessary Conditions for Nonprincipal Polarizations in Galois Extensions

Let K be a Galois CM-field of degree 4 with maximal totally real subfield K_0 and primitive CM-type Φ. Let m be a positive integer. Let $\mathfrak{c}$ be a fractional ideal of K. We want to prove some necessary conditions for $\Phi(\mathfrak{c})$ to admit a polarization of type $(1, m)$. In this section we will make repeated use of the Kronecker symbol $\left(\frac{\cdot}{\cdot}\right)$. We note that since K is Galois and has a primitive CM-type Φ by 2.2.6 it is a cyclic extension of $\mathbb{Q}$. Let $\mathrm{Gal}(K/\mathbb{Q}) = \langle s \rangle$ be the Galois group of K over $\mathbb{Q}$. We then have that there are four CM-types on K:

$$\Phi_1 = \{1_K, s\},$$
$$\Phi_2 = \left\{1_K, s^3\right\},$$
$$\Phi_3 = \left\{s^2, s^3\right\},$$
$$\Phi_4 = \left\{s^2, s\right\}.$$

Note that s^2 is complex conjugation and $\overline{\Phi}_1 = \Phi_3$ and $\overline{\Phi}_2 = \Phi_4$ so that there are two equivalence classes of CM-type represented by Φ_1 and Φ_2.

THEOREM 3.3.1. *Let K be a quartic cyclic number field. Let K_0 be its unique quadratic subfield. Then $K_0 = \mathbb{Q}(\sqrt{\mathrm{Disc}_{K/\mathbb{Q}}})$ and there exists some $t \in \mathbb{Z}$ such that $\mathrm{Disc}_{K/\mathbb{Q}} = t^2 \mathrm{Disc}_{K_0/\mathbb{Q}}$.*

PROOF. The proof relies on a result which comes from a paper by Edgar and Peterson ([**2**]). It follows from their calculations in proving Proposition 2 that $\mathrm{Disc}_{K/\mathbb{Q}} = w^2 f^3$ for some integers w and f with f squarefree and $K_0 = \mathbb{Q}(\sqrt{f})$. The fact that $K_0 = \mathbb{Q}(\sqrt{\mathrm{Disc}_{K/\mathbb{Q}}})$ follows immediately from that. From this it follows that

$$\sqrt{\mathrm{Disc}_{K/\mathbb{Q}}} = a + b\sqrt{\mathrm{Disc}_{K_0/\mathbb{Q}}}$$

for some rational numbers a and b. Then

$$\mathrm{Disc}_{K/\mathbb{Q}} = a^2 + b^2 \mathrm{Disc}_{K_0/\mathbb{Q}} + 2ab\sqrt{\mathrm{Disc}_{K_0/\mathbb{Q}}}.$$

This implies that $2ab = 0$ as $\mathrm{Disc}_{K/\mathbb{Q}}$ is rational. Now, b cannot be 0 so $a = 0$. Thus $\mathrm{Disc}_{K/\mathbb{Q}} = b^2 \mathrm{Disc}_{K_0/\mathbb{Q}}$. By [**4**] page 443 we know $\mathrm{Disc}^2_{K_0/\mathbb{Q}}$ divides $\mathrm{Disc}_{K/\mathbb{Q}}$ which implies that b is an integer. □

THEOREM 3.3.2. *Let K be a number field and $\mathrm{Disc}_{K/Q}$ the discriminant of K. The rational primes p which ramify in K are precisely those which divide $\mathrm{Disc}_{K/\mathbb{Q}}$.*

PROOF. A proof can be found in any introduction to algebraic number theory, for instance in [**10**] chapter 3, section 2. □

THEOREM 3.3.3. *Let K be a number field of degree n. Let p be a rational prime which does not divide* $\mathrm{Disc}_{K/\mathbb{Q}}$. *Let r be the number of distinct primes of $\mathfrak{O}_K$ lying over p. We have the following equality:*

$$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = (-1)^{n-r}.$$

PROOF. This is a famous result of Stickelberger and a proof can be found in [**4**] on page 502, in section 4 of chapter 26. □

PROPOSITION 3.3.4. *Let K be a Galois CM-field of degree 4 with maximal totally real subfield K_0 and primitive CM-type Φ. Let m be a positive integer. Let $\mathfrak{c}$ be a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Assume that L admits a Riemann form inducing a polarization of type $(1, m)$. Then for every prime p dividing m which is unramified in K,*

$$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{p}\right) = 1.$$

PROOF. Since L admits a Riemann form inducing a polarization of type $(1, m)$ by Theorem 3.1.2 there is an element $\mathfrak{a} = \prod_{q|m} \mathfrak{a}_q$ in $R_m(K)$ such that $\mathfrak{c}\bar{\mathfrak{c}}D\mathfrak{a} = (\delta)$ where $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$. Then since p is unramified in K, $\mathfrak{a}_p$ satisfies either (1) or (3) of Theorem 3.1.2. So $f = ef \leqslant 2$ where $e = e(\mathfrak{p}|p)$ and $f = f(\mathfrak{p}|p)$ where $\mathfrak{p}$ is any prime of K lying over p. Let r be the number of primes lying over p. As K is Galois, $erf = 4$. It follows that $r = 2$ or 4. Thus by Theorem 3.3.3,

$$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = 1.$$

That $\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{p}\right)$ follows from Theorem 3.3.1. This completes the proof. □

PROPOSITION 3.3.5. *Let K be a primitive quartic Galois CM-field with cyclic Galois group* $\mathrm{Gal}(K/\mathbb{Q}) = \langle s \rangle$. *Let $K_0 = \mathbb{Q}(\sqrt{n})$, $n \in \mathbb{Q}$ be the real quadratic subfield of K. Let $\Phi = \{\phi_1, \phi_2\}$ be a CM-type on K. Let $\delta \in K^\times$. Then the following are equivalent:*

(1) *$\delta \in K_\Phi(i\mathbb{R})$, i.e. $\overline{\phi_1(\delta)} = -\phi_1(\delta)$ and $\overline{\phi_2(\delta)} = -\phi_2(\delta)$.*
(2) *$s^2(\delta) = -\delta$.*
(3) *$\mathrm{Tr}^K_{K_0}(\delta) = 0$.*
(4) *$\mathrm{Tr}^K_{\mathbb{Q}}(\delta) = \mathrm{Tr}^K_{\mathbb{Q}}((1 + \sqrt{n})\delta) = 0$.*
(5) *$\mathrm{Tr}^K_{\mathbb{Q}}(\delta) = Tr^K_{\mathbb{Q}}(\alpha\delta) = 0$ where $\alpha \in K_0$ is any element such that $K_0 = \mathbb{Q}(\alpha)$.*

PROOF. We prove that (1) implies (2). Assume (1) holds. Then considering all CM-types on K we can assume that one of ϕ_1 and ϕ_2 are s or s^3. Assume that $\phi_1 = s$. Then by assumption $= -s(\delta)$. We also have that s^2 is complex conjugation. Thus

$$s^2(s(\delta)) = -s(\delta)$$

$$s^3(\delta) = -s(\delta)$$
$$s^2(\delta) = -\delta.$$

Now assume that $\phi_1 = s^3$. So

$$\overline{s^3(\delta)} = -s^3(\delta)$$
$$s^5(\delta) = -s^3(\delta)$$
$$s^2(\delta) = -\delta.$$

This proves (2).

We now prove (2) implies (1). Assume (2) holds. As in the proof that (1) implies (2) we can assume $\phi_1 = s$ or $\phi_1 = s^3$. Without loss of generality assume $\phi_1 = s$.

$$\begin{aligned}\overline{\phi_1(\delta)} &= \overline{s(\delta)} \\ &= s^3(\delta) \\ &= s(-\delta) \\ &= -s(\delta) \\ &= -\phi_1(\delta).\end{aligned}$$

Now, because of the possible CM-types on K we can assume $\phi_2 = 1_K$ or $\phi_2 = s^3$. Assume $\phi_2 = 1_K$. Then

$$\begin{aligned}\overline{\phi_2(\delta)} &= \overline{\delta} \\ &= s^2(\delta) \\ &= -\delta \\ &= -\phi_2(\delta).\end{aligned}$$

Assume $\phi_2 = s^3$. Then

$$\begin{aligned}\overline{\phi_2(\delta)} &= \overline{s^3(\delta)} \\ &= s^5(\delta) \\ &= s^3(-\delta) \\ &= -s^3(\delta) \\ &= -\phi_2(\delta).\end{aligned}$$

This proves (1).

We now prove (2) is equivalent to (3). Note that as K_0 is totally real, the only automorphism of K over K_0 is conjugation, which is s^2. The result follows from this.

That (3) implies (4) follows immediately from the facts that $\mathrm{Tr}_{\mathbb{Q}}^{K} = \mathrm{Tr}_{\mathbb{Q}}^{K_0} \circ \mathrm{Tr}_{K_0}^{K}$ and that $1 + \sqrt{n} \in K_0$.

We prove (4) implies (3). Assume $\mathrm{Tr}_{\mathbb{Q}}^{K}(\delta) = \mathrm{Tr}^{\mathbb{Q}}((1+\sqrt{n})\delta) = 0$. Let $\mathrm{Tr}_{K_0}^{K}(\delta) = a + b\sqrt{n}$ with $a, b, \in \mathbb{Q}$.

$$\begin{aligned} 0 &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\delta) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(\mathrm{Tr}_{K_0}^{K}(\delta)) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(a + b\sqrt{n}) \\ &= 2a. \end{aligned}$$

This implies $a = 0$. Similarly,

$$\begin{aligned} 0 &= \mathrm{Tr}_{\mathbb{Q}}^{K}((1+\sqrt{n})\delta) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(\mathrm{Tr}_{K_0}^{K}((1+\sqrt{n})\delta)) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}((1+\sqrt{n})\,\mathrm{Tr}_{K_0}^{K}(\delta)) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}((1+\sqrt{n})b\sqrt{n}) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K}(b\sqrt{n} + bn) \\ &= 2bn. \end{aligned}$$

This implies $b = 0$ which proves (3).

That (3) implies (5) follows immediately from the facts that $\mathrm{Tr}_{\mathbb{Q}}^{K} = \mathrm{Tr}_{\mathbb{Q}}^{K_0} \circ \mathrm{Tr}_{K_0}^{K}$ and that α and $1 + \alpha \in K_0$.

We prove (5) implies (3). Let $\mathrm{Tr}_{K_0}^{K}(\delta) = a + b\sqrt{n}$ with $a, b \in \mathbb{Q}$. It follows that $a = 0$ for the same reasons as in the proof that (4) implies (3). Let $\alpha = c + d\sqrt{n}$ with $c, d \in \mathbb{Q}$. Then

$$\begin{aligned} 0 &= \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha\delta) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(\alpha\,\mathrm{Tr}_{K_0}^{K}(\delta))) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}((c+d\sqrt{n})b\sqrt{n}) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{K_0}(cb\sqrt{n} + bdn) \\ &= 2bdn. \end{aligned}$$

So $0 = 2bdn$. Since $d \neq 0$ and $n \neq 0$, $b = 0$, as required. □

Corollary 3.3.6. *Let K be a Galois CM-field of degree 4 with maximal totally real subfield K_0 and primitive CM-type Φ. Let m be a positive integer. Let $\mathfrak{c}$ be a fractional ideal of K and $L = \Phi(\mathfrak{c})$. Suppose that L admits a polarization of type $(1, m)$ which is induced by $\delta \in K$ which is such that $\delta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$ so that $(\delta) = \mathfrak{c}\bar{\mathfrak{c}}\,\mathrm{Diff}_{K/\mathbb{Q}}\,\mathfrak{a}$ as in*

Theorem 3.1.2. Let p be a prime dividing m. Suppose that p ramifies in K. Then $\mathfrak{a}_p$ satisfies one of (2), (4), (5), or (6) and we have the following possibilities.

(1) *If p splits in $\mathfrak{O}_{K_0}$, then $\mathfrak{a}_p$ satisfies (2) or (6)(b).*
(2) *If p is inert in $\mathfrak{O}_{K_0}$ then $\mathfrak{a}_p$ satisfies (5).*
(3) *If p ramifies in $\mathfrak{O}_{K_0}$ then $\mathfrak{a}_p$ satisfies (4).*

PROOF. Let r be the number of primes of $\mathfrak{O}_K$ lying over p and let e and f be the common ramification index and inertia degree respectively of any prime lying over p in $\mathfrak{O}_K$.

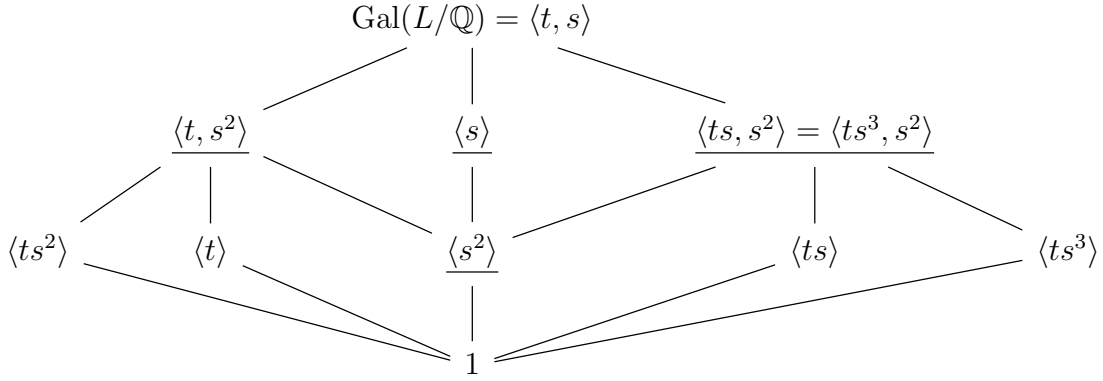
Suppose p splits in $\mathfrak{O}_{K_0}$. Then because $erf = 4$ and we know $r \geqslant 2$, so we must have $ef \leqslant 2$. We also know that p ramifies so that $e = 2$ and thus $f = 1$. This implies that $\mathfrak{a}_p$ satisfies one of (2) or (6)(b).

Suppose p is inert in $\mathfrak{O}_{K_0}$. Then $f \geqslant 2$. Because p ramifies in $\mathfrak{O}_K$, $e \geqslant 2$, so $e = 2$ and $f = 2$. This implies $\mathfrak{a}_p$ satisfies (5).

Suppose p ramifies in $\mathfrak{O}_{K_0}$. So $e \geqslant 2$. We have $e = 4$ or $e = 2$. Assume $e = 2$. We will obtain a contradiction. Let $\mathfrak{p}$ be any prime of K lying above p and let T be the inertia field of $\mathfrak{p}$. By Theorem 28 in [**7**] we have that $[K : T] = e = 2$, so $T = K_0$. But also by Theorem 28 of [**7**], p is unramified in $T = K_0$ which is a contradiction. So $e = 4$. Thus $\mathfrak{a}_p$ satisfies (4). □

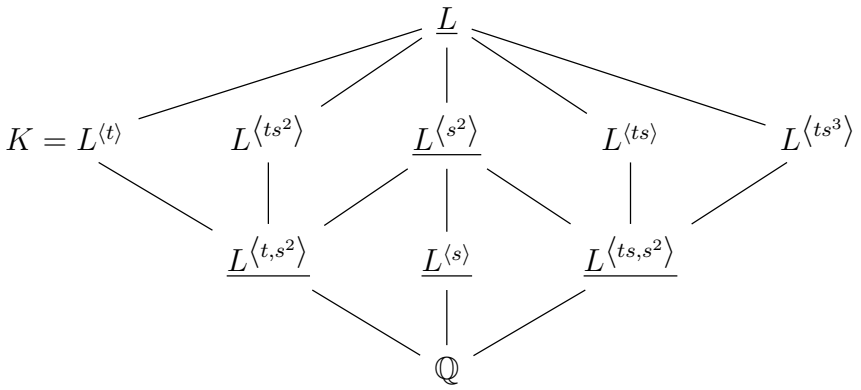
3.4. Necessary Conditions for Non-Galois Extensions

Let K be a CM-field, K_0 its maximal totally real subfield, Φ a CM-type on K, and L the Galois closure of K. In this section we will assume that K is not Galois. We consider the case in which K is a quartic CM-field. In this case as noted in Example 2.2.6, since K is non-Galois, L is a degree 8 extension with Galois group D_8. We use the presentation of D_8 given by $\langle t, s \,|\, t^2 = s^4 = 1\rangle$. We have the following diagram of subgroups:



The normal subgroups are underlined. By the fundamental theorem of Galois theory, the diagram of subfields of L is the same diagram inverted. There are five quartic subfields. One of them is totally real, but the others are totally imaginary extensions of a quadratic

real subfield, so any of them could be taken to be our field K. We choose $K = L^{\langle t \rangle}$ and $K_0 = L^{\langle t, s^2 \rangle}$. So we get the following diagram of subfields of L:



In this situation, s^2 restricts to complex conjugation on any of the quartic CM-fields. The embeddings of K into $\mathbb{C}$ are the restrictions of $\{1, s, s^2, s^3\}$. In the rest of this section we will denote $\sigma = s|_K$. The above notation will be fixed for the entire section.

Lemma 3.4.1. *We have*

$$s(K) = s^3(K) = L^{\langle ts^2 \rangle}, \qquad s^2(K) = K. \tag{3.4.1}$$

Proof. Let $x \in K$. Then

$$ts^2(sx) = ts^3x = ts^3tx = sx.$$

It follows that $sx \in L^{\langle ts^2 \rangle}$; this implies that $s(K) = L^{\langle ts^2 \rangle}$. The remaining claims in (3.4.1) have a similar proof. □

The totally real quadratic extension K_0 of $\mathbb{Q}$ contained in K is $L^{\langle t, s^2 \rangle}$. The set of all CM-types of $K/\mathbb{Q}$ is $\{\{1, \sigma\}, \{1, \sigma^3\}, \{\sigma^2, \sigma\}, \{\sigma^2, \sigma^3\}\}$. The elements of $\mathrm{Gal}(L/\mathbb{Q})$ acts on the set of embeddings of K into $\mathbb{C}$ by composition on the left. We have the following

table of the actions of $\mathrm{Gal}(L/\mathbb{Q})$ on $1, \sigma, \sigma^2, \sigma^3$.

	1	σ	σ^2	σ^3
1	1	σ	σ^2	σ^3
s	σ	σ^2	σ^3	1
s^2	σ^2	σ^3	1	σ
s^3	σ^3	1	σ	σ^2
t	1	σ^3	σ^2	σ
ts	σ^3	σ^2	σ	1
ts^2	σ^2	σ	1	σ^3
ts^3	σ	1	σ^3	σ^2

We therefore obtain the following table of actions on the CM-types:

	$\{1,\sigma\}$	$\{1,\sigma^3\}$	$\{\sigma^2,\sigma\}$	$\{\sigma^2,\sigma^3\}$
1	$\{1,\sigma\}$	$\{1,\sigma^3\}$	$\{\sigma^2,\sigma\}$	$\{\sigma^2,\sigma^3\}$
s	$\{\sigma^2,\sigma\}$	$\{1,\sigma\}$	$\{\sigma^2,\sigma^3\}$	$\{1,\sigma^3\}$
s^2	$\{\sigma^2,\sigma^3\}$	$\{\sigma^2,\sigma\}$	$\{1,\sigma^3\}$	$\{1,\sigma\}$
s^3	$\{1,\sigma^3\}$	$\{\sigma^2,\sigma^3\}$	$\{1,\sigma\}$	$\{\sigma^2,\sigma\}$
t	$\{1,\sigma^3\}$	$\{1,\sigma\}$	$\{\sigma^2,\sigma^3\}$	$\{\sigma^2,\sigma\}$
ts	$\{\sigma^2,\sigma^3\}$	$\{1,\sigma^3\}$	$\{\sigma^2,\sigma\}$	$\{1,\sigma\}$
ts^2	$\{\sigma^2,\sigma\}$	$\{\sigma^2,\sigma^3\}$	$\{1,\sigma\}$	$\{1,\sigma^3\}$
ts^3	$\{1,\sigma\}$	$\{\sigma^2,\sigma\}$	$\{1,\sigma^3\}$	$\{\sigma^2,\sigma^3\}$

Therefore, we have the following stabilizers:

(3.4.2)

CM-type	stabilizer
$\{1,\sigma\}$	$\{1,ts^3\}$
$\{\sigma^2,\sigma^3\}$	$\{1,ts^3\}$
$\{1,\sigma^3\}$	$\{1,ts\}$
$\{\sigma^2,\sigma\}$	$\{1,ts\}$

LEMMA 3.4.2. *Let Φ be a CM-type for K, and let K^r be the reflex field of K with respect to Φ. We have:*

(3.4.3)

Φ	K^r
$\{1, \sigma\}$	$L^{\langle ts^3 \rangle}$
$\{\sigma^2, \sigma^3\}$	$L^{\langle ts^3 \rangle}$
$\{1, \sigma^3\}$	$L^{\langle ts \rangle}$
$\{\sigma^2, \sigma\}$	$L^{\langle ts \rangle}$

PROOF. By definition, the reflex field of K with respect to Φ is the fixed field in L of the stabilizer in $\mathrm{Gal}(L/\mathbb{Q})$ of Φ. The table (3.4.3) now follows immediately from (3.4.2). □

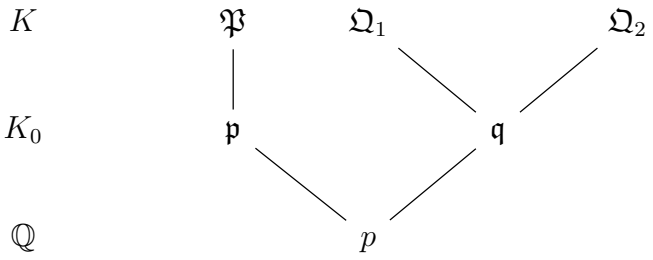
We have the following result.

LEMMA 3.4.3. *Let $K_0 = \mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Q}$. Let $\{\sigma_1, \sigma_2\}$ be a CM-type for $K/\mathbb{Q}$. Let $\delta \in K$. Then the following are equivalent*

(1) $\overline{\sigma_1(\delta)} = -\sigma_1(\delta)$ *and* $\overline{\sigma_2(\sigma)} = -\sigma_2(\delta)$.
(2) $s^2(\delta) = -\delta$.
(3) $\mathrm{Tr}^K_{K_0}(\delta) = 0$.
(4) $\mathrm{Tr}^K_{\mathbb{Q}}(\delta) = \mathrm{Tr}^K_{\mathbb{Q}}((1 + \sqrt{n})\delta) = 0$.
(5) $\mathrm{Tr}^K_{\mathbb{Q}}(\delta) = \mathrm{Tr}^K_{\mathbb{Q}}(\alpha\delta) = 0$ *where $\alpha \in K_0$ is such that $K_0 = \mathbb{Q}(\alpha)$.*

PROOF. The proof of this is nearly identical to the proof of Proposition 3.3.5. Instead of s being an automorphism of K, s is an automorphism of L but this does not change any of the calculations. □

In future results we will have occasion to consider primes with a factorization of the following form in K:



where $\mathfrak{P}$ is not ramified over $\mathfrak{p}$. Note that this implies that $f(\mathfrak{P}|p) = 2$ and that this is only possible in a non-Galois extension as the inertia degrees do not agree between primes.

LEMMA 3.4.4. *Let p be a rational prime unramified in K which decomposes in K in the above manner, that is, $p\mathfrak{O}_K = \mathfrak{P}\mathfrak{Q}_1\mathfrak{Q}_2$ where $\mathfrak{P} = \mathfrak{p}\mathfrak{O}_K$ for a prime $\mathfrak{p}$ of $\mathfrak{O}_{K_0}$ above p and $\mathfrak{q}\mathfrak{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2$ for a prime $\mathfrak{q}$ of $\mathfrak{O}_{K_0}$. Then p is unramified in L.*

PROOF. Note that as L is Galois, the ramification index for each prime of L above p are the same number e. Let r be the number of primes of L above p and let f be the residue degree common to each of them. We have $erf = 8$ as L is degree 8. We also know that $f \geqslant 2$ as $\mathfrak{P}$ already has inertia degree 2 in K. Also, as p has already factored into three primes in K we have $r \geqslant 3$. But $r < 8$, so the only possibility is $r = 4$, $f = 2$ and $e = 1$. □

LEMMA 3.4.5. *Let Φ be a CM-type on K. Let K^r be the reflex field with respect to Φ and K_0^r the maximal totally real subfield of K^r. Let p be a rational prime that is unramified in L. Let k and n be positive integers such that kn is even. Let $\mathfrak{C}$ be a fractional ideal of K with norm v^2, for v a rational number, and let $\mathfrak{B}$ be an ideal of K. Let $\delta \in K^\times$. Assume that*

$$s^2(\delta) = -\delta, \tag{3.4.4}$$

$$\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{B}) = p^n, \tag{3.4.5}$$

$$(\delta) = \mathfrak{C}\,\mathrm{Diff}_{K/\mathbb{Q}}\mathfrak{B}^{-k}. \tag{3.4.6}$$

Then

(1) *$\delta s(\delta) \notin \mathbb{Q}$ and $\mathrm{Disc}_{K/\mathbb{Q}}$ is not a square in $\mathbb{Z}$.*
(2) *$\delta s(\delta) \in K_0^r$ and $K_0^r = \mathbb{Q}(\delta s(\delta))$.*
(3) *$K_0^r = \mathbb{Q}(\sqrt{\mathrm{Disc}_{K/\mathbb{Q}}})$.*
(4) *$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{p}\right)$.*

PROOF. Since kn is even, there exists $\ell \in \mathbb{Z}$ such that $-kn = 2\ell$.

Proof of (1). Applying the norm map of ideals to (3.4.6) we obtain the following equality of ideals:

$$(\mathrm{N}_{\mathbb{Q}}^K(\delta)) = (v^2\,\mathrm{Disc}_{K/\mathbb{Q}}\,p^{-kn}). \tag{3.4.7}$$

It follows that there exists $\varepsilon \in \{\pm 1\}$ such that

$$\mathrm{N}_{\mathbb{Q}}^K(\delta) = \varepsilon v^2\,\mathrm{Disc}_{K/\mathbb{Q}}\,p^{-kn}. \tag{3.4.8}$$

Now

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^K(\delta) &= \delta s(\delta)s^2(\delta)s^3(\delta)\\ &= \delta s(\delta)(-\delta)s(-\delta)\\ &= (\delta s(\delta))^2. \end{aligned}\tag{3.4.9}$$

By (3.4.8) and (3.4.9) we have

$$(\delta s(\delta))^2 = \varepsilon v^2 \operatorname{Disc}_{K/\mathbb{Q}} p^{-kn}. \tag{3.4.10}$$

Now

$$\begin{aligned} \overline{\delta s(\delta)} &= s^2(\delta s(\delta)) \\ &= s^2(\delta)s^3(\delta) \\ &= (-\delta)(-s(\delta)) \\ &= \delta s(\delta). \end{aligned} \tag{3.4.11}$$

From (3.4.11) we conclude that $\delta s(\delta) \in \mathbb{R}$ so that $(\delta s(\delta))^2 > 0$; since v^2, $\operatorname{Disc}_{K/\mathbb{Q}}$, and p^{-kn} are all positive, we see that $\varepsilon = 1$ and so

$$(\delta s(\delta))^2 = v^2 \operatorname{Disc}_{K/\mathbb{Q}} p^{-kn}. \tag{3.4.12}$$

Assume that $\delta s(\delta) \in \mathbb{Q}$; we will obtain a contradiction. Since $\delta s(\delta) \in \mathbb{Q}$ we have:

$$\begin{aligned} \delta s(\delta) &= s(\delta s(\delta)) \\ &= s(\delta)s^2(\delta) \\ &= -\delta s(\delta). \end{aligned} \tag{3.4.13}$$

From (3.4.13) we have $\delta s(\delta) = 0$, so that $\delta = 0$, a contradiction. Next, assume that $\operatorname{Disc}_{K/\mathbb{Q}}$ is a square in $\mathbb{Z}$; we will obtain a contradiction. Let $\operatorname{Disc}_{K/\mathbb{Q}} = d_0^2$ where $d_0 \in \mathbb{Z}$. By (3.4.12) we now have

$$(\delta s(\delta))^2 = (v d_0 p^{\ell})^2. \tag{3.4.14}$$

Then (3.4.14) implies that $\delta s(\delta) = \pm v d_0 p^{\ell}$; in particular, $\delta s(\delta) \in \mathbb{Q}$, which is a contradiction.

Proof of (2). We have $K_0^r = L^{\langle ts, s^2 \rangle}$. Now

$$\begin{aligned} t(\delta s(\delta)) &= t(\delta)ts(\delta) \\ &= \delta tst(\delta) \\ &= \delta s^3(\delta) \\ &= -\delta s(\delta). \end{aligned} \tag{3.4.15}$$

And:

$$\begin{aligned} s(\delta s(\delta)) &= s(\delta)s^2(\delta) \\ &= -\delta s(\delta). \end{aligned} \tag{3.4.16}$$

By (3.4.15) and (3.4.16) we have $ts(\delta s(\delta)) = \delta s(\delta)$ and $s^2(\delta s(\delta)) = \delta s(\delta)$. This implies that $\delta s(\delta) \in K_0^r$. Since $\delta s(\delta) \notin \mathbb{Q}$ by i) and $[K_0 : \mathbb{Q}] = 2$, we conclude that $K_0 = \mathbb{Q}(\delta s(\delta))$.

Proof of (3). From (3.4.12) we have

$$\delta s(\delta) = \pm v p^{\ell} \sqrt{\mathrm{Disc}_{K/\mathbb{Q}}}. \tag{3.4.17}$$

By (2) we obtain $K_0^r = \mathbb{Q}(\sqrt{\mathrm{Disc}_{K/\mathbb{Q}}})$.

Proof of (4). Let $K_0^r = \mathbb{Q}(\sqrt{m})$ where m is a square-free integer. Since $\mathrm{Disc}_{K/\mathbb{Q}}$ is not a square in $\mathbb{Z}$, so by (3) there exists an integer c such that $c^2 m = \mathrm{Disc}_{K/\mathbb{Q}}$. Since p is unramified in K by assumption, $p \nmid \mathrm{Disc}_{K/\mathbb{Q}}$; this implies that $p \nmid c$. Therefore, $\left(\frac{c}{p}\right)$ is not zero and is hence ± 1. It follows that

$$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{c^2 m}{p}\right) = \left(\frac{c}{p}\right)^2 \left(\frac{m}{p}\right) = \left(\frac{m}{p}\right).$$

We have

$$\mathrm{Disc}_{K_0^r/\mathbb{Q}} = \begin{cases} 4m & \text{if } m \equiv 2, 3 \pmod 4, \\ m & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

It follows that

$$\left(\frac{m}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{p}\right) \tag{3.4.18}$$

if $m \equiv 1 \pmod 4$. We claim that (3.4.18) also holds if $m \equiv 2, 3 \pmod 4$. Assume that $m \equiv 2, 3 \pmod 4$. By assumption, p is unramified in L; this implies that p is unramified in K_0^r. It follows that $p \nmid \mathrm{Disc}_{K_0^r/\mathbb{Q}} = 4m$. In particular, $p \neq 2$. We have

$$\left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{p}\right) = \left(\frac{4m}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{m}{p}\right) = \left(\frac{m}{p}\right).$$

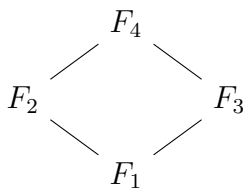
This proves our claim. We now have

$$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{p}\right).$$

This completes the proof. □

Let K_1/K_2 be an extension of number fields and let $\mathfrak{P}$ be a prime of K_1. Then we will denote the prime $\mathfrak{P} \cap \mathfrak{O}_{K_2}$ of K_2 that $\mathfrak{P}$ lies over by $\mathfrak{P}_{K_2}$.

Lemma 3.4.6. *Let F_1, F_2, F_3, and F_4 be number fields with subfield relationships illustrated by the following diagram.*



Assume $F_4 = F_2F_3$, and F_3 is a normal extension of F_1. Let $\mathfrak{P}$ be a prime of F_4, and assume that $\mathfrak{P}_{F_1}$ is unramified in F_4. Then

$$f(\mathfrak{P}_{F_4}/\mathfrak{P}_{F_2}) \leqslant f(\mathfrak{P}_{F_3}/\mathfrak{P}_{F_1}). \tag{3.4.19}$$

PROOF. This follows from Ex. 10, Chap. 4, p. 83 and Theorem 28 of Chap. 4 of [**7**]. □

THEOREM 3.4.7. *Let Φ be a CM-type on K. Let K^r be the reflex field with respect to Φ and K_0^r the maximal totally real subfield of K^r. Let $\mathfrak{c}$ be a fractional ideal of K. Let L be the Galois closure of K. Let m be a positive integer. Let p be a prime dividing m. Assume that p is unramified in L, and that $\mathbb{C}^2/\Phi(\mathfrak{c})$ admits a polarization of type $(1, m)$. By Theorem 3.1.2 there exists $\mathfrak{a} = \prod_{q|m} \mathfrak{a}_q$ in $R_m(K)$ and $\delta \in K_\Phi(i\mathbb{R}_{>0})$ such that*

$$(\delta) = \mathfrak{c}\bar{\mathfrak{c}}\mathrm{Diff}_{K/\mathbb{Q}} \prod_{q|m} \mathfrak{a}_q. \tag{3.4.20}$$

Then $\mathrm{Disc}_{K/\mathbb{Q}}$ is not a square in $\mathbb{Z}$ and exactly one of the following cases holds:

(3.4.21)

$\mathfrak{a}_p$ *satisfies*	r	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{p}\right)$	r'	$\left(\frac{\mathrm{Disc}_{K^r/\mathbb{Q}}}{p}\right)$	$\left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{p}\right)$
(1)	2	1	1	2	1	1
(1)	3	−1	1	2	1	−1
(3)	4	1	1	4	1	1
(3)	3	−1	1	2	1	−1

Here, r and r' are the number of primes of K and K^r lying over p, respectively, and (1) and (3) refer to conditions in Theorem 3.1.2.

PROOF. To begin we note that in this proof we will sometimes use the Stickelberger criterion 3.3.3 without further comment.

By Theorem 3.1.2, since p is unramified in K, $\mathfrak{a}_p$ must satisfy (1) or (3) of Theorem 3.1.2. For brevity, in the remainder of this proof, if $\mathfrak{a}_p$ satisfies (1) of Theorem 3.1.2, then we will say that (1) holds; a similar comment applies if $\mathfrak{a}_p$ satisfies (3) of Theorem 3.1.2. We define an ideal $\mathfrak{B}$ of K as follows. If (1) holds, then there exists a prime $\mathfrak{P}$ of K lying over p such that $\mathfrak{a}_p = \mathfrak{P}^{-k}$ with $e(\mathfrak{P}/p) = 1$ and $f(\mathfrak{P}/p) = 2$; in this case we define $\mathfrak{B} = \mathfrak{P}$. If (3) holds, then there exist distinct prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of K lying over p such that $\mathfrak{a}_p = \mathfrak{P}_1^{-k}\mathfrak{P}_2^{-k}$ with $e(\mathfrak{P}_1/p) = e(\mathfrak{P}_2/p) = 1$ and $f(\mathfrak{P}_1/p) = f(\mathfrak{P}_2/p) = 1$; in this case define $\mathfrak{B} = \mathfrak{P}_1\mathfrak{P}_2$. We then have $(\delta) = \mathrm{Diff}_{K/\mathbb{Q}}\mathfrak{B}^{-k}$ and $\mathrm{N}_Q^K(\mathfrak{B}) = p^2$. We also note that by Lemma 3.4.3 we have $s^2(\delta) = -\delta$. We note that $\mathrm{Disc}_{K/\mathbb{Q}}$ is not a square in $\mathbb{Z}$ by Lemma 3.4.5. By Lemma 3.4.5 we also have $\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{p}\right)$. Since p is

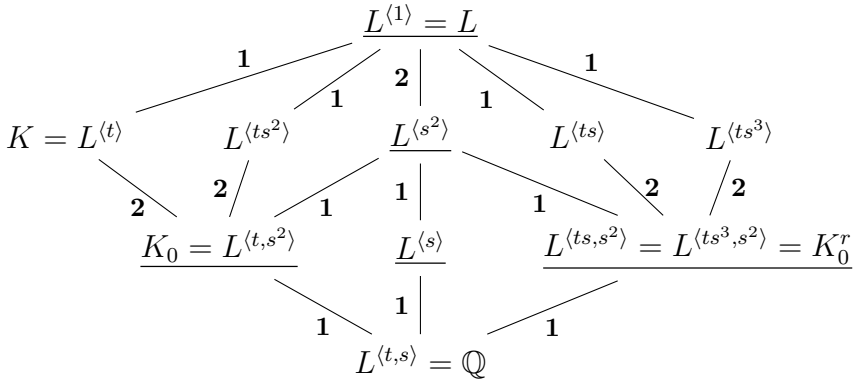


FIGURE 1. Inertial degrees for any prime of L lying over p when (1) holds and $(\mathrm{Disc}_{K/\mathbb{Q}}/p) = 1$.

unramified in K, p must split in K_0 by Corollary 3.2.3; hence, $\left(\mathrm{Disc}_{K_0/\mathbb{Q}}/p\right) = 1$. We have $\left(\mathrm{Disc}_{K/\mathbb{Q}}/p\right) = (-1)^{4-r} = (-1)^r$ and $\left(\mathrm{Disc}_{K^r/\mathbb{Q}})/p\right) = (-1)^{4-r'} = (-1)^{r'}$.

Assume that (1) holds and that $\left(\mathrm{Disc}_{K/\mathbb{Q}}/p\right) = 1$. Since $\left(\mathrm{Disc}_{K/\mathbb{Q}}/p\right) = 1$ we see that r is even. Hence, $r = 2$ or $r = 4$. If $r = 4$, then $f(\mathfrak{P}/p) = 1$, a contradiction. Hence, $r = 2$. Let $\mathfrak{R}$ be any prime of L lying over p. Then the inertial degrees of all the intermediate quadratic extensions are as in fig. 1. This may be proven as follows. $f(\mathfrak{R}_{K_0}/p) = 1$: use $\left(\mathrm{Disc}_{K_0/\mathbb{Q}}/p\right) = 1$. $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{L^{\langle s\rangle}}) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{K_0^r}) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_L/\mathfrak{R}_{L^{\langle ts^3\rangle}}) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_L/\mathfrak{R}_{L^{\langle ts\rangle}}) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_{K_0^r}/\mathfrak{R}_{\mathbb{Q}}) = 1$: use $\left(\mathrm{Disc}_{K_0^r/\mathbb{Q}}/p\right) = 1$. $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{K_0}) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_L/\mathfrak{R}_{L^{\langle ts^2\rangle}}) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_L/\mathfrak{R}_K) = 1$: use Lemma 3.4.6. $f(\mathfrak{R}_{L^{\langle s\rangle}}/\mathfrak{R}_{\mathbb{Q}}) = 1$: use multiplicativity. $f(\mathfrak{R}_K/\mathfrak{R}_{K_0}) = 2$: use $r = 2$. All remaining inertial degrees now follow from multiplicativity. From fig. 1 we conclude that in $L^{\langle ts\rangle}$ there are exactly two primes lying over p; similarly, in in $L^{\langle ts^3\rangle}$ there are exactly two primes lying over p. Since $K^r = L^{\langle ts\rangle}$ or $K^r = L^{\langle ts^3\rangle}$ it follows that $r' = 2$ and $(\mathrm{Disc}_{K^r/\mathbb{Q}})/p = 1$.

Assume that (1) holds and that $(\mathrm{Disc}_{K/\mathbb{Q}}/p) = -1$. Since $(\mathrm{Disc}_{K/\mathbb{Q}}/p) = -1$ we see that r is odd. Hence, $r = 1$ or $r = 3$. If $r = 1$, then $4 = e(\mathfrak{P}/p)f(\mathfrak{P}/p) = 2$, a contradiction. Hence, $r = 3$. Since there are three primes of K lying over p, since $f(\mathfrak{P}/p) = 2$, since p is unramified in L, and since L is a degree eight Galois extension of $\mathbb{Q}$, we see that there are exactly four primes of L lying over p. Let $\mathfrak{R}$ be any prime of L lying over p. Then $f(\mathfrak{R}/p) = 2$, and the inertial degrees of some intermediate quadratic extensions are as in fig. 2. These numbers are obtained as follows. $f(\mathfrak{R}_{K_0}/\mathfrak{R}_{\mathbb{Q}}) = 1$: use that p splits in K_0. $f(\mathfrak{R}_{K_0^r}/\mathfrak{R}_{\mathbb{Q}}) = 2$: use $(\mathrm{Disc}_{K_0^r/\mathbb{Q}}/p) = -1$. $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{K_0^r}) = 1$, $f(\mathfrak{R}_{L^{\langle ts\rangle}}/\mathfrak{R}_{K_0^r}) = 1$, $f(\mathfrak{R}_{L^{\langle ts^3\rangle}}/\mathfrak{R}_{K_0^r}) = 1$, $f(\mathfrak{R}_L/\mathfrak{R}_{L^{\langle s^2\rangle}}) = 1$, $f(\mathfrak{R}_L/\mathfrak{R}_{L^{\langle ts\rangle}}) = 1$, $f(\mathfrak{R}_L/\mathfrak{R}_{L^{\langle ts^3\rangle}}) = 1$: use $f(\mathfrak{R}_{K_0^r}/\mathfrak{R}_{\mathbb{Q}}) = 2$, $f(\mathfrak{R}/p) = 2$, and multiplicativity. $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{L^{\langle s\rangle}}) = 1$: use Lemma

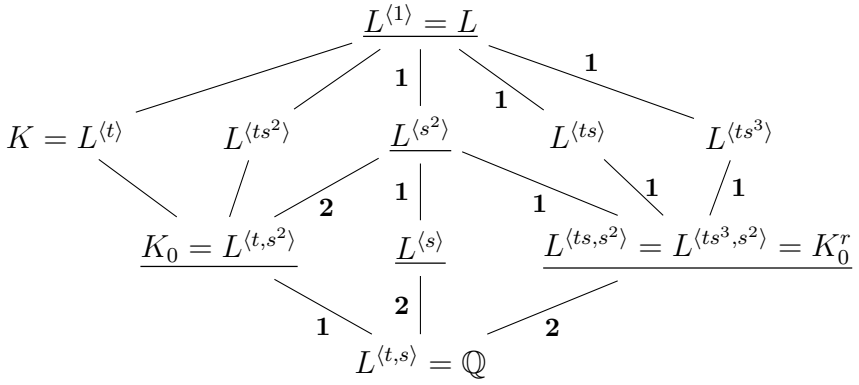


FIGURE 2. Some inertial degrees for any prime of L lying over p when (1) or (3) holds and $(\mathrm{Disc}_{K/\mathbb{Q}}/p)) = -1$.

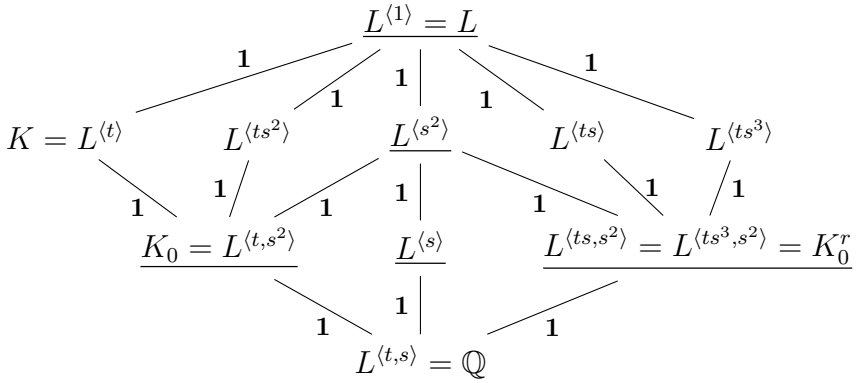


FIGURE 3. Inertial degrees for any prime of L lying over p when (3) holds and $(\mathrm{Disc}_{K/\mathbb{Q}}/p) = 1$.

3.4.6. $f(\mathfrak{R}_{L^{\langle s\rangle}}/\mathfrak{R}_{\mathbb{Q}}) = 2$, $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{K_0}) = 2$: use multiplicativity. From fig. 2 we conclude that there are exactly two primes of $L^{\langle ts\rangle}$ lying over p; similarly, there are exactly two primes of $L^{\langle ts^3\rangle}$ lying over p. It follows that $r' = 2$ and $(\mathrm{Disc}_{K^r/\mathbb{Q}})/p) = 1$.

Assume that (3) holds and that $(\mathrm{Disc}_{K/\mathbb{Q}}/p) = 1$. Since $(\mathrm{Disc}_{K/\mathbb{Q}}/p) = 1$, we have $r = 2$ or $r = 4$. If $r = 2$, then $4 = e(\mathfrak{P}_1/p)f(\mathfrak{P}_1/p) + e(\mathfrak{P}_2/p)f(\mathfrak{P}_2/p) = 1 + 1 = 2$, a contradiction. Hence, $r = 4$. Let $\mathfrak{R}$ be any prime of L lying over p. Then the inertial degrees of all the intermediate quadratic extensions are as in fig. 3. These numbers are computed as follows. $f(\mathfrak{R}_{K_0}/p) = 1$: use that p splits in K_0. $f(\mathfrak{R}_{K_0^r}/p) = 1$: use $1 = (\mathrm{Disc}_{K/\mathbb{Q}}/p) = (\mathrm{Disc}_{K_0/\mathbb{Q}}/p)$. $f(\mathfrak{R}_K/\mathfrak{R}_{K_0}) = 1$: use $r = 4$, so that $f(\mathfrak{R}_K/p) = 1$, and multiplicativity. $f(\mathfrak{R}_{L^{\langle s^2\rangle}}/\mathfrak{R}_{K_0}) = f(\mathfrak{R}_L/\mathfrak{R}_K) = 1$: use Lemma 3.4.6. We now have $f(\mathfrak{R}/p) = 1$ by multiplicativity; all the remaining inertial degrees now follow from multiplicativity. From fig. 3 we see that p splits into four distinct primes in both $L^{\langle ts}$ and $L^{\langle ts^3\rangle}$; this implies that $r' = 4$ and $(\mathrm{Disc}_{K^r/\mathbb{Q}}/p) = 1$.

Finally, assume that (3) holds and that $(\mathrm{Disc}_{K/\mathbb{Q}}\,/p) = -1$. Since $(\mathrm{Disc}_{K/\mathbb{Q}}\,/p) = -1$ we have $r = 1$ or $r = 3$. We cannot have $r = 1$ since by (3) the integer r is at least 2. Hence, $r = 3$. Let $\mathfrak{P}_3$ be the third prime of K lying over p. We then have

$$4 = e(\mathfrak{P}_1/p)f(\mathfrak{P}_1/p) + e(\mathfrak{P}_2/p)f(\mathfrak{P}_2/p) + e(\mathfrak{P}_3/p)f(\mathfrak{P}_3/p) = 1 + 1 + f(\mathfrak{P}_3/p).$$

This implies that $f(\mathfrak{P}_3/p) = 2$. Since there are three primes of K lying over p, since $f(\mathfrak{P}_3/p) = 2$, since p is unramified in L, and since L is a degree eight Galois extension of $\mathbb{Q}$, we see that there are exactly four primes lying over p. Let $\mathfrak{R}$ be any prime of L lying over p. Then $f(\mathfrak{R}/p) = 2$, and the inertial degrees of some intermediate quadratic extensions are as in fig. 2; the arguments for these degrees are as in the case when (1) holds and $(\mathrm{Disc}_{K/\mathbb{Q}}\,/p) = -1$. From fig. 2 we conclude that there are exactly two primes of $L^{\langle ts \rangle}$ lying over p; similarly, there are exactly two primes of $L^{\langle ts^3 \rangle}$ lying over p. It follows that $r' = 2$ and $(\mathrm{Disc}_{K^r/\mathbb{Q}}\,/p) = 1$. □

Chapter 4: Algorithms and Calculations

Let K be a quartic primitive CM-field with CM-type Φ. Let $\mathfrak{c}$ be a fractional ideal of K and let $L = \Phi(\mathfrak{c})$. Let m be a positive integer. In this chapter we write an algorithm determining whether $\mathbb{C}^2/L$ admits a polarization of type $(1, m)$. We also present explicit code in the language PARI GP which implements this algorithm. In addition we present two applications of this algorithm. First we compile some descriptive statistics about the frequency of polarizations. Next we give some illustrations of the necessary conditions which we have proven in the previous chapter.

4.1. The Algorithm

Input: A CM-field K with maximal totally real subfield K_0 such that K does not contain a strict CM-subfield. A fractional ideal $\mathfrak{c}$ of K. A positive integer m.

Output: An element δ, totally imaginary and such that the imaginary part of $\phi(\delta)$ is positive for each $\phi \in \Phi$ which determines a polarization of type $(1.m)$ on L, if possible. If this is not possible, the output is the string "A polarization of type $(1, m)$ is not possible".

(1) Factor m into prime powers $m = \prod_{i=1}^{t} p_i^{v_{p_i}(m)}$.
(2) For each $j \in \{1, \ldots, t\}$, factor the ideal (p_j) into prime ideals in K. Algorithms for this already exist.
(3) Determine whether there exists an $j \in \{1, \ldots, t\}$ such that there are only prime ideals $\mathfrak{p}$ in the decomposition of p_j which enable the possibility of ideals $\mathfrak{a}_p$ satisfying the conditions in 3.1.2. If any such prime appears in the decomposition of m, output "A polarization of type $(1, m)$ is not possible". If there are no such primes in the decomposition of m then proceed to next step.
(4) Calculate the different D_K of K.
(5) For each prime p dividing m, let $A(p)$ be the collection of ideals of the form $\mathfrak{a}_p$ where $\mathfrak{a}_p$ satisfies one of the conditions in Theorem 3.1.2.
(6) Enumerate the collection S_m of ideals of the form

$$\mathfrak{b} = \mathfrak{c}\bar{\mathfrak{c}} D_K \prod_{p|m} \mathfrak{a}_p$$

where for each p, $\mathfrak{a}_p$ is a selection of some element of $A(p)$.

(7) For each element $\mathfrak{b}$ of S_m, determine whether $\mathfrak{b}$ is principal. If no element is principal, output "A polarization of type $(1, m)$ is not possible". Otherwise, select an ideal $\mathfrak{b}$ which is principal and a generator δ.

(8) Calculate $\mathrm{Re}(\phi(\delta))$ for each $\phi \in \Phi$. If this is positive for each ϕ, output δ. Otherwise, output "A polarization of type $(1, m)$ is not possible".

That this algorithm is sufficient relies on the assumption that K has only ± 1 as roots of unity, so that all the units of K are real units. This is justified by the fact that K is a primitive CM-field. This is okay in our circumstances because we are assuming that K is primitive from which it follows that K contains no roots of unity other than ± 1 so that Lemma 2.2.9 applies.

In order to use the above algorithm to obtain data we implemented it in the PARI programming language. The code for this implementation is given below.

```
Beginning_Check(K, m) =
{
    /* This is a function which checks whether necessary conditions
    for a polarization to occur are satisfied. If a given number
    field fails this check there is no reason to continue the
    algorithm.*/

    \\ We iterate the check over all the primes dividing m
    for(n=1,#factor(m)~,
    p = factor(m)[n, 1];
    v_p = factor(m)[n, 2];
    r = #idealfactor(K,p)~;
    for(t=1, r,
        e = idealfactor(K,p)[t,1][3];
        f = idealfactor(K,p)[t,1][4];
        \\ We will only consider the check to be failed if
        \\every prime lyingabove some prime factor of m fails
        \\the required condition so weinitialize a variable
        \\"index" to count the number of primes that fail.
        index = 0;
        if(v_p > 1,
            if((e> 1 && f > 1), index++,
                if(f>3, index++)
            )
        );
        if(index == r, return(0))
        );
    );
    return(1)
};
```

```
Find_Admissible_Aps(K,m) =
{
    /*This is a function which calculates the ideals a_p given in
    the main theorem, if they exist.*/
    \\We want to produce a list of the ideals which may satisfy
    \\the theorem. We do this by starting with an empty list and
    \\adding potential ideals as we go.
    list = [];
    for(n=1, #factor(m)~,
        \\For each prime p dividing m we determine all the a_ps
        \\if any that exist.
        a_plist = [];
        p = factor(m)[n, 1];
        \\We will repeatedly use the factorization of p in K
        \\so we initialize a variable for it.
        pfactor = idealfactor(K,p);
        v_p = factor(m)[n, 2];
        r = #pfactor~;
        for(t=1, r,
            e = pfactor[t,1][3];
            f = pfactor[t,1][4];
            \\This is case (1) of the main theorem.
            if(e == 1 && f == 2,
            a_plist = concat(a_plist, [idealpow(K, pfactor[t,1],-v_p)])
            );
            \\This is case (2) of the main theorem.
            if(e == 2 && f == 1,
            a_plist = concat(a_plist, [idealpow(K, pfactor[t,1],-2*v_p)])
            );
            \\This is case (3) of the main theorem. This one has
            \\two prime ideals involved in it so we have
            \\ to include a nested for loop. Nested for loops will
            \\appear for every case which involves multiplication for
            \\two prime ideals.
            if((e == 1 && f == 1) && t < r,
            for(s=t+1, r,
                if (pfactor[s,1][3] == 1 && pfactor[s,1][4] == 1,
                a_plist = concat(a_plist, [idealmul(K,idealpow(K, pfactor[t,1],-v_p),
                idealpow(K,pfactor[s,1],-v_p))])
                );
            );
            );
```

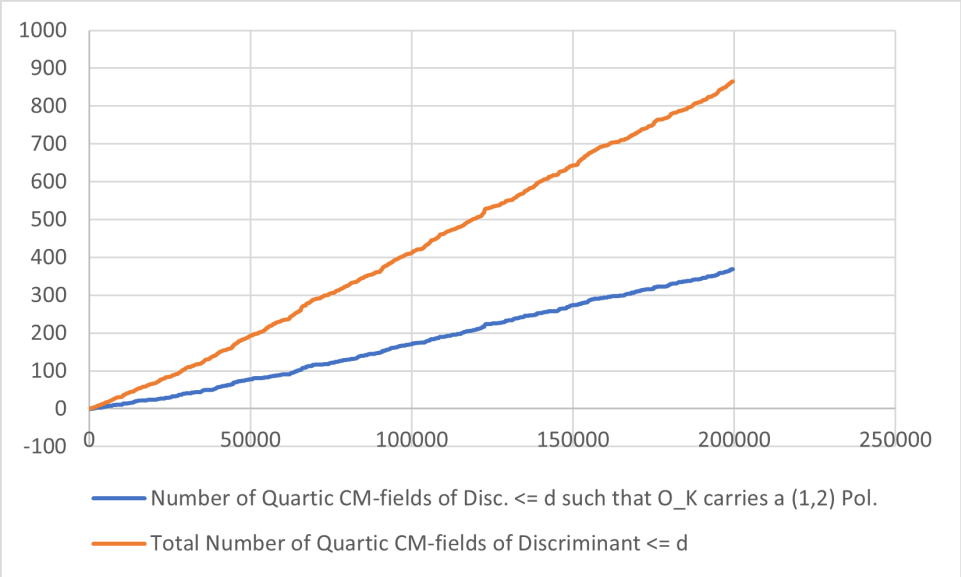
```
\\This is case (4) of the main theorem.
if((v_p == 1 && (e == 4 && f == 1)) || (v_p == 1 && (e == 3 && f == 1)),
a_plist = concat(a_plist, [idealpow(K, pfactor[t,1],-2)])
);
\\This is case (5) of the main theorem.
if(v_p == 1 && (e == 2 && f == 2),
a_plist = concat(a_plist, [idealpow(K, pfactor[t,1],-1)])
);
\\The remaining code covers case (6).
\\This is more complicated
\\because there are two different
\\configurations of e and f in some of them so I've
\\written two conditionsals for (a) and (c).
\\ We first look at (6)(a).
if(v_p == 1 && e == 3 && f == 1 && t < r,
for(s=t+1, r,
    if (pfactor[s,1][3] == 1 && pfactor[s,1][4] == 1,
    a_plist = concat(a_plist, [idealmul(K,idealpow(K, pfactor[t,1],-v_p),
    idealpow(K,pfactor[s,1],-v_p))])
    );
);
);
if(v_p == 1 && e == 1 && f == 1 && t < r,
for(s=t+1, r,
    if (pfactor[s,1][3] == 3 && pfactor[s,1][4] == 1,
    a_plist = concat(a_plist, [idealmul(K,idealpow(K, pfactor[t,1],-v_p),
    idealpow(K,pfactor[s,1],-v_p))])
    );
);
);
\\Case (6)(b).
if(v_p == 1 && e == 2 && f == 1 && t < r,
for(s=t + 1, r,
    if (pfactor[s,1][3] == 2 && pfactor[s,1][4] == 1,
    a_plist = concat(a_plist, [idealmul(K,idealpow(K, pfactor[t,1],-v_p),
    idealpow(K,pfactor[s,1],-v_p))])
    );
);
);
\\Case (6)(c).
if(v_p == 1 && e == 2 && f == 1 && t < r,
    for(s=t + 1, r,
    a_plist = concat(a_plist, [idealmul(K,idealpow(K, pfactor[t,1],-v_p),
```

```
                idealpow(K,pfactor[s,1],-v_p))])
                );
            );
            if(v_p == 1 && e == 1 && f == 1 && t < r,
            for(s=t + 1, r,
                if (pfactor[s,1][3] == 2 && pfactor[s,1][4] == 1,
                a_plist = concat(a_plist, [idealmul(K,idealpow(K, pfactor[t,1],-v_p),
                idealpow(K,pfactor[s,1],-v_p))])
                );
            );
            );
        );
        \\We add all the lists of a_p factors to the main list.
        list = concat(list, [a_plist]);
    );
    \\We output the list of lists of a_ps.
    return(list)
};

FindS(K, m) =
{
    /*This is a function which takes
    the a_p factors found in the last
    function and multiplies them
    to find the set S_m given in the
    main theorem. This amounts to
    calculating each possible product
    \prod a_p as p runs over the prime
    factors of m. */
    \\There is a Pari function called
    \\fold which will perform a function
    \\f(x_1,x__2, ..., x_n) on all
    \\elements of the n-fold cartesian
    \\product of a collection
    \\of sets.
    Aplistm = concat(Find_Admissible_Aps(K, m), [[K.diff]]);
    S = fold((A, B) ->[idealmul(K, a, b)|a<-A;b<-B], Aplistm);
    return(S)
};

FindPrincipal(K,m) =
{
    /*This function determines whether any of the ideals
```

```
    in S_m are principal ideals. The output is the set of
    pairs of principal elements of S_m together with a generator.*/
    IdealSet = FindS(K,m);
    PrincipalSet = [];
    for(n=1, #IdealSet~,
        Ideal = IdealSet[n];
        \\We use the function bnfisprincipal. The first entry of this
        \\function outputs a vector which is 0 if and only
        \\if the ideal which was input is principal. We
        \\have to use a workaround for the if
        \\statement because if the classgroup is trivial
        \\ it outputs the empty vector.
        gen = bnfisprincipal(K, Ideal);
        if(0 * gen[1] == gen[1],
        PrincipalSet = concat(PrincipalSet,[[Ideal, gen[2]]]);
        );
    );
    return(PrincipalSet);
};

IsGenIm(K, m) =
{
    /*This function determines whether the generators of the principal ideals in S_m
    are generated by imaginary elements. The output is the set of such ideals.*/

ProspSet = FindPrincipal(K, m);
ImSet = [];
for(n=1, #ProspSet~,
        if(nfelttrace(K, ProspSet[n][2]*nfsubfields(K, 2)[1][2]) == 0
        && nfelttrace(K, ProspSet[n][2]) == 0,
        ImSet = concat(ImSet, [ProspSet[n]])
        );
);
    return(ImSet)
};
ListCheck(Fields, Polalist) =
{
    /*This is a function which inputs a list of fields and a list of
    integers and checks whether they fields ring of integers admits
    a polarization of type (1, m) for each m in Pola.*/

    Outlist = [];
    \\We don't need all of the data given by LMFDB so we only save
```

```
    \\some of their output in our output list. What we save is the
    \\LMFDB label of the field, a defining polynomial, and the
    \\ discriminant.
for(n=1,#Fields~,
Outlist = concat(Outlist, [[Fields[n][1],Fields[n][2],
            Fields[n][3]]])
);
    \\We iterate through each field, calculate and output all
    \\the data we want.
    for(n=1, #Fields~,
        F = bnfinit(Fields[n][2]);
        Outlist[n] = concat(Outlist[n], [F.clgp.no]);
        \\We enumerate over our list of polarizations and check
        \\whether F has a polarization by each of them.
        for(t=1, #Polalist~,
            P = Polalist[t];
            if(Beginning_Check(F, P) == 0,
            \\An output of B means "Beginning Check Failure"
            Outlist[n] = concat(Outlist[n], ["B"]),
            if(FindS(F, P) == [],
            \\An output of A means "No choices of Ap for some p"
            Outlist[n] = concat(Outlist[n], ["A"]),
            \\An Output of P means
            \\"No choice of c \overline c D_K \prod a_p is principal.
            if(FindPrincipal(F, P) == [],
            Outlist[n] = concat(Outlist[n], ["P"]),
            \\An Output of I means
            \\"No choice of c \overline c D_K \prod a_p
            \\has an imaginary generator.
            if(IsGenIm(F, P) == [],
            Outlist[n] = concat(Outlist[n], ["I"]),
            \\If F has a polarization of type (1, P), output 1.
            Outlist[n] = concat(Outlist[n], [1]);
            ););););
        );
    );
    return(Outlist)
}
```

FIGURE 4. How many number fields K of less than a given discriminant are such that $\mathfrak{O}_K$ admits a polarization of type (1,2).



4.2. Descriptive Statistics

In this section we compile some information about how often a given primitive quartic CM-field K has a ring of integers $\mathfrak{O}_K$ which admits a polarization of type (1, p) for a given prime. Let $C(d)$ be the number of primitive quartic CM-fields of discriminant less than or equal to d. Let $C(d,p)$ be the number of primitive quartic CM-fields of discriminant less than or equal to d for which $\mathfrak{O}_K$ admits a polarization of type $(1,p)$.

Remarkably, for all the p that we have considered both $C(d)$ and $C(d,p)$ for fixed p appear linear in d for $d \leqslant 200,000$. Evidence for this is provided in Figures 4, 5 and 6 for the primes $p = 2, p = 3$ and $p = 5$. In Table 4.1 we list the apparent ratio $C(d,p)/C(d)$ for several primes p. In addition, the graphs of $C(d,p)$ also appear linear for all the primes $p \leqslant 1223$. We don't yet have an explanation for this or a proof that it continues to hold.

4.3. Composite Types

We also considered the following question: Given a primitive CM-field K, a CM-type Φ, a fractional ideal $\mathfrak{c}$ of K and a square-free semiprime number $m = pq$, for p and q distinct primes, is there any relationship between whether $\Phi(\mathfrak{c})$ admits a polarization of type $(1,p)$ and a polarization of type $(1,q)$ and whether it admits a polarization of type $(1,pq)$. There is some relationship that can be easily ascertained. For instance, if there does not exist a polarization of type $(1,p)$ or $(1,q)$ for the reason that the ideals $\mathfrak{a}_p$ or $\mathfrak{a}_q$, as described in Theorem 3.1.2 do not exist, then there can be no polarization of type

FIGURE 5. How many number fields K of less than a given discriminant are such that $\mathfrak{O}_K$ admits a polarization of type (1,3).

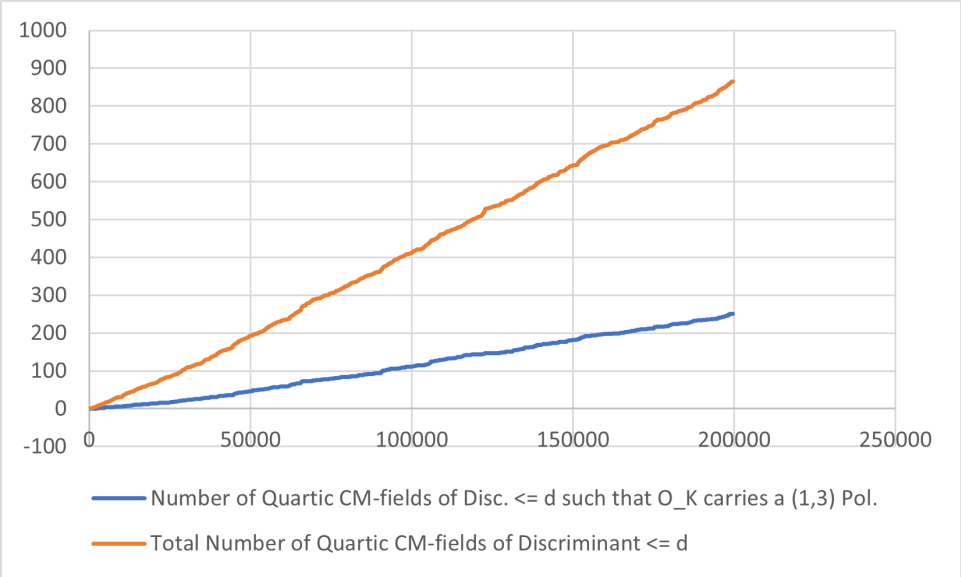
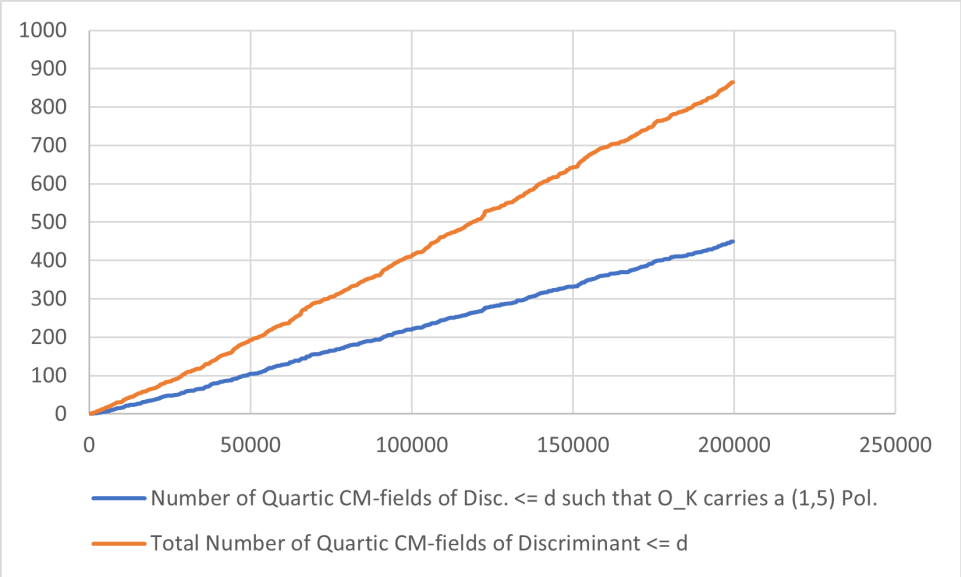


FIGURE 6. How many number fields K of less than a given discriminant are such that $\mathfrak{O}_K$ admits a polarization of type (1,5).



$(1, pq)$ for the same reason. However one might ask whether in the case that $\mathfrak{a}_p$ and $\mathfrak{a}_q$ exist does the existence of a polarization on $\Phi(\mathfrak{c})$ of type $(1, p)$ and another polarization of type $(1, q)$ guarantee the existence of a polarization of type $(1, pq)$? The answer is "no", although counterexamples are very infrequent. One example is the field K labeled 4.0.105125.1 in the L-Functions and Modular Forms Database, which is generated over $\mathbb{Q}$ by a root of the polynomial $x^4 - 2x^3 + 14x^2 - 13x + 6$. This field is such that $\mathfrak{O}_K$

TABLE 4.1. A table of proportions of the number of quartic CM-fields up to discriminant d with a (1, p) polarization over the total number of fields up to discriminant d.

2	3	5	7	11	13	17	19	23	29
0.4230	0.2831	0.5217	0.2816	0.5537	0.2531	0.3768	0.5347	0.4147	0.5811
31	37	41	43	47	53	59	61	67	71
0.6704	0.1908	0.6915	0.2167	0.4288	0.2268	0.6485	0.6218	0.1661	0.7756
73	79	83	89	97	101	103	107	109	113
0.3520	0.7377	0.2536	0.7232	0.3371	0.6404	0.3902	0.2502	0.5852	0.3210
127	131	137	139	149	151	157	163	167	173
0.3905	0.6698	0.2958	0.5951	0.5763	0.7395	0.2724	0.0971	0.3921	0.2026
179	181	191	193	197	199	211	223	227	229
0.6793	0.6437	0.8695	0.3568	0.1132	0.7559	0.5832	0.3345	0.1945	0.6137
233	239	241	251	257	263	269	271	277	281
0.3382	0.8171	0.7648	0.7105	0.3831	0.4706	0.6040	0.7321	0.2541	0.7316

admits a polarization of type $(1,2)$ and a polarization of type $(1,3)$ but does not admit a polarization of type $(1,6)$. This is the only field we found with this property for $2,3$ and 6. One explanation for the relative infrequency of this occurence is that if the different $\mathrm{Diff}_{K/\mathbb{Q}}$ happens to be principal, generated by some $\delta_0 \in K_\Phi(i\mathbb{R})$ and we have for some $\delta_2, \delta_3 \in K_\Phi(i\mathbb{R})$,

$$(\delta_2) = \delta_0 \mathfrak{a}_2,$$

and

$$(\delta_3) = \delta_0 \mathfrak{a}_3,$$

then we have

$$(\delta_0^{-1}\delta_2\delta_3) = \delta_0 \mathfrak{a}_2 \mathfrak{a}_3.$$

Note that $\delta_0^{-1}\delta_2\delta_3$ will be in $K_\Psi(i\mathbb{R})$ for some CM-type Ψ. Thus under these circumstances there is a polarization of type $(1,6)$. It turns out that it is very common for a quartic CM-field to have a principal different, generated by an imaginary element.

4.4. Illustration of Necessary Conditions

Galois Fields. In this subsection we illustrate the results in Section 3.3 on Galois extensions. In particular we want to show illustrations of Proposition 3.3.4. In the following tables, we list several CM-fields K for which $\mathfrak{O}_K$ admits a polarization of type $(1,p)$ where p is a prime given in the table. The fields are described both by a label given to them by the L-functions and Modular Forms Data Base (LMFDB) as well as by a polynomial $f(x)$ such that K is generated over $\mathbb{Q}$ by a root of $f(x)$. We also give the discriminant of each field. Table 4.2 contains fields K for which $\mathfrak{O}_K$ admits a polarization

TABLE 4.2. An illustration of Proposition 3.3.4 with $p = 2$.

Label	Polynomial	Discriminant	$\left(\frac{\text{Disc}_{K/\mathbb{Q}}}{2}\right)$	$\left(\frac{\text{Disc}_{K_0/\mathbb{Q}}}{2}\right)$
4.0.3501153.1	$x^4 - x^3 + 46x^2 - 105x + 951$	3501153	1	1
4.0.47071057.1	$x^4 - x^3 + 192x^2 - 397x + 9857$	47071057	1	1
4.0.44720977.1	$x^4 - x^3 + 158x^2 + 685x + 2073$	44720977	1	1
4.0.8214057.1	$x^4 - x^3 + 61x^2 + 297x + 618$	8214057	1	1
4.0.64701513.1	$x^4 - x^3 + 121x^2 - 567x + 5934$	64701513	1	1
4.0.87528825.2	$x^4 - x^3 + 265x^2 - 543x + 17814$	87528825	1	1
4.0.19061833.1	$x^4 - x^3 + 119x^2 - 251x + 4236$	19061833	1	1
4.0.84311993.1	$x^4 - x^3 + 555x^2 + x + 73492$	84311993	1	1
4.0.94924073.1	$x^4 - x^3 + 589x^2 + x + 82706$	94924073	1	1
4.0.99139625.1	$x^4 - x^3 + 301x^2 - 1231x + 7426$	99139625	1	1

TABLE 4.3. An illustration of Proposition 3.3.4 with $p = 3$.

Label	Polynomial	Discriminant	$\left(\frac{\text{Disc}_{K/\mathbb{Q}}}{3}\right)$	$\left(\frac{\text{Disc}_{K_0/\mathbb{Q}}}{3}\right)$
4.0.19061833.1	$x^4 - x^3 + 119x^2 - 251x + 4236$	19061833	1	1
4.0.44720977.1	$x^4 - x^3 + 158x^2 + 685x + 2073$	44720977	1	1
4.0.47071057.1	$x^4 - x^3 + 192x^2 - 397x + 9857$	47071057	1	1
4.0.14602768.1	$x^4 + 97x^2 + 388$	14602768	1	1
4.0.6224272.1	$x^4 + 73x^2 + 1168$	6224272	1	1
4.0.58411072.1	$x^4 + 194x^2 + 1552$	58411072	1	1
4.0.24897088.1	$x^4 + 146x^2 + 4672$	24897088	1	1
4.0.92416000.4	$x^4 + 380x^2 + 32490$	92416000	1	1
4.0.43264000.4	$x^4 + 260x^2 + 15210$	43264000	1	1
4.0.12544000.2	$x^4 + 140x^2 + 4410$	12544000	1	1

of type $(1, 2)$. Note that In every case $\left(\frac{\text{Disc}_{K/\mathbb{Q}}}{2}\right) = \left(\frac{\text{Disc}_{K_0/\mathbb{Q}}}{2}\right) = 1$, as expected because of Proposition 3.3.4. Tables 4.2 and Table 4.3 illustrate the same fact for the primes 3 and 5.

Whether $p = 2, 3$ or 5 we have $\left(\frac{\text{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\text{Disc}_{K_0/\mathbb{Q}}}{p}\right) = 1$ as expected. This is a small collection of data but we have run the same calculations on hundreds of Galois fields and for many more primes and always seen the same result.

We now look at similar data to examine the question whether the necessary condition is given in Proposition 3.3.4 is a sufficient condition for $\mathfrak{O}_K$ to admit a polarization of type $(1, p)$. It is not a sufficient condition. The following tables show fields K for which $\mathfrak{O}_K$ does not admit a polarization of type $(1, p)$ for $p = 2, 3$ and 5 that nonetheless

TABLE 4.4. An illustration of Proposition 3.3.4 with $p = 5$.

Label	Polynomial	Discriminant	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{5}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{5}\right)$
4.0.65597509.1	$x^4 - x^3 + 252x^2 - 774x + 11097$	65597509	1	1
4.0.38359789.2	$x^4 - x^3 + 191x^2 - 591x + 6705$	38359789	1	1
4.0.5929741.1	$x^4 - x^3 + 23x^2 - 215x + 975$	5929741	1	1
4.0.74618461.1	$x^4 - x^3 + 53x^2 + 763x + 4557$	74618461	1	1
4.0.1295029.1	$x^4 - x^3 + 14x^2 + 34x + 393$	1295029	1	1
4.0.42508549.1	$x^4 - x^3 + 44x^2 - 240x + 4203$	42508549	1	1
4.0.226981.1	$x^4 - x^3 + 8x^2 - 42x + 117$	226981	1	1
4.0.10061824.1	$x^4 + 68x^2 + 306$	10061824	1	1
4.0.10061824.2	$x^4 + 68x^2 + 850$	10061824	1	1
4.0.14526784.2	$x^4 + 122x^2 + 2196$	14526784	1	1

TABLE 4.5. An illustration of the insufficiency of the Jacobi symbol condition for polarizations of type $(1, 2)$.

Label	Polynomial	Discriminant	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{2}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{2}\right)$
4.0.13456625.2	$x^4 - x^3 + 106x^2 + 4x + 3656$	13456625	1	1
4.0.33229625.2	$x^4 - x^3 + 171x^2 + 4x + 8596$	33229625	1	1
4.0.99139625.2	$x^4 - x^3 + 301x^2 + 4x + 24716$	99139625	1	1
4.0.27437625.2	$x^4 - x^3 + 91x^2 + 9x + 3996$	27437625	1	1
4.0.56984625.2	$x^4 - x^3 + 116x^2 - 821x + 3601$	56984625	1	1
4.0.2471625.2	$x^4 - x^3 + 41x^2 + 4x + 796$	2471625	1	1

satisfy $\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{p}\right) = \left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{p}\right) = 1$. It is interesting to note that although none of these fields had a polarization of type $(1, p)$, there always existed an ideal $\mathfrak{a}_p$ as given in Theorem 3.1.2. The nonexistence of a polarization was always because the fractional ideal $\mathrm{Diff}_{K/\mathbb{Q}}\,\mathfrak{a}_p$ always failed to be a principal fractional ideal. This is expected. Indeed, by Theorem 3.2.1 there exists a fractional ideal $\mathfrak{c}$ of K and a CM-type Φ such that $\Phi(\mathfrak{c})$ admits a polarization of type $(1, p)$.

Non-Galois Fields. In this subsection we illustrate the results in Section 3.4 on Galois extensions. In particular we want to show illustrations of Proposition 3.4.7. In the following tables, we list several CM-fields K for which $\mathfrak{O}_K$ admits a polarization of type $(1, p)$ where p is a prime given in the table. The fields are described both by a label given to them by the L-functions and Modular Forms Data Base (LMFDB) as well as by a polynomial $f(x)$ such that K is generated over $\mathbb{Q}$ by a root of $f(x)$. We also give the discriminant of each field. Table 4.8 contains fields K for which $\mathfrak{O}_K$ admits a polarization of type $(1, 2)$. Note that In every case the number of primes above p in K as well as the Kronecker symbols mentioned in Theorem 3.4.7 are as expected. Tables 4.8

TABLE 4.6. An illustration of the insufficiency of the Jacobi symbol condition for polarizations of type $(1,3)$.

Label	Polynomial	Discriminant	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{3}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{3}\right)$
4.0.48778000.3	x^4+145x^2+2320	48778000	1	1
4.0.48778000.2	x^4+145x^2+5220	48778000	1	1
4.0.49948672.4	x^4+116x^2+2842	49948672	1	1
4.0.73984000.2	x^4+340x^2+2890	73984000	1	1
4.0.30976000.2	x^4+220x^2+1210	30976000	1	1
4.0.92416000.2	x^4+380x^2+3610	92416000	1	1
4.0.43264000.2	x^4+260x^2+1690	43264000	1	1
4.0.12544000.1	x^4+140x^2+490	12544000	1	1
4.0.256000.4	x^4+20x^2+10	256000	1	1
4.0.39304000.1	x^4+170x^2+340	39304000	1	1
4.0.88121125.2	$x^4-x^3+56x^2+584x+5971$	88121125	1	1
4.0.12008989.1	$x^4-x^3+29x^2+415x+933$	12008989	1	1
4.0.88121125.1	$x^4-x^3+56x^2-1196x+4191$	88121125	1	1
4.0.614125.1	$x^4-x^3+11x^2-101x+171$	614125	1	1

TABLE 4.7. An illustration of the insufficiency of the Jacobi symbol condition for polarizations of type $(1,5)$.

Label	Polynomial	Discriminant	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{5}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{5}\right)$
4.0.40495104.3	x^4+156x^2+234	40495104	1	1
4.0.12008989.1	$x^4-x^3+29x^2+415x+933$	12008989	1	1
4.0.4499456.1	x^4+52x^2+26	4499456	1	1

TABLE 4.8. An illustration of Proposition 3.4.7 with $p=2$.

Label	Polynomial	Discriminant	Case	r	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{2}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{2}\right)$	r'	$\left(\frac{\mathrm{Disc}_{K^r/\mathbb{Q}}}{2}\right)$	$\left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{2}\right)$
4.0.3757.1	$x^4-2x^3+6x^2-5x+2$	3757	(3)	3	-1	1	2	1	-1
4.0.8405.1	$x^4-2x^3+8x^2-7x+2$	8405	(3)	3	-1	1	2	1	-1
4.0.29189.1	$x^4-2x^3+8x^2-7x+8$	29189	(3)	3	-1	1	2	1	-1
4.0.40293.1	$x^4-2x^3+8x^2-7x+4$	40293	(3)	3	-1	1	2	1	-1
4.0.62197.1	$x^4-x^3+3x^2+14x+32$	62197	(3)	3	-1	1	2	1	-1
4.0.63869.1	$x^4-2x^3+10x^2-9x+16$	63869	(3)	3	-1	1	2	1	-1
4.0.66181.1	$x^4-2x^3+16x^2-15x+18$	66181	(3)	3	-1	1	2	1	-1
4.0.93925.1	$x^4-x^3+17x^2-19x+106$	93925	(3)	3	-1	1	2	1	-1
4.0.39593.1	$x^4-x^3+10x^2-7x+49$	39593	(1)	2	1	1	2	1	1
4.0.74273.1	$x^4-2x^3+13x^2-12x+19$	74273	(1)	2	1	1	2	1	1
4.0.25721.1	$x^4-2x^3+11x^2-10x+8$	25721	(3)	4	1	1	4	1	1

and Table 4.9 illustrate the same fact for the primes 3 and 5. Whether $p=2,3$ or 5 we have that the necessary conditions of Theorem 3.4.7 are satisfied. This is a small

TABLE 4.9. An illustration of Proposition 3.4.7 with $p = 3$.

Label	Polynomial	Discriminant	Case	r	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{3}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{3}\right)$	r'	$\left(\frac{\mathrm{Disc}_{K^r/\mathbb{Q}}}{2}\right)$	$\left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{2}\right)$
4.0.90944.1	$x^4 - 2x^3 + 4x^2 + 4x + 18$	90944	(3)	3	-1	1	2	1	-1
4.0.25088.1	$x^4 + 6x^2 + 2$	25088	(3)	3	-1	1	2	1	-1
4.0.42632.1	$x^4 + 9x^2 + 2$	42632	(3)	3	-1	1	2	1	-1
4.0.26533.1	$x^4 - x^3 + 9x^2 - 19x + 23$	26533	(1)	2	1	1	2	1	1
4.0.30589.1	$x^4 - x^3 + 6x^2 + 2x + 17$	30589	(1)	2	1	1	2	1	1
4.0.63037.1	$x^4 - 2x^3 + 16x^2 - 15x + 27$	63037	(3)	4	1	1	4	1	1
4.0.52897.1	$x^4 - x^3 + 8x^2 + x + 27$	52897	(3)	4	1	1	4	1	1
4.0.56953.1	$x^4 - x^3 + 11x^2 - 20x + 36$	56953	(3)	4	1	1	4	1	1
4.0.99937.1	$x^4 - x^3 + 2x^2 + 13x + 21$	99937	(3)	4	1	1	4	1	1

TABLE 4.10. An illustration of Proposition 3.4.7 with $p = 5$.

Label	Polynomial	Discriminant	Case	r	$\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{5}\right)$	$\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{5}\right)$	r'	$\left(\frac{\mathrm{Disc}_{K^r/\mathbb{Q}}}{5}\right)$	$\left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{5}\right)$
4.0.98192.2	$x^4 - 2x^3 + 15x^2 - 14x + 30$	98192	(3)	3	-1	1	2	1	-1
4.0.27648.1	$x^4 + 6x^2 + 3$	27648	(3)	3	-1	1	2	1	-1
4.0.32832.1	$x^4 - 2x^3 + 3x^2 + 4x + 10$	32832	(3)	3	-1	1	2	1	-1
4.0.78057.3	$x^4 - x^3 + 12x^2 + 23x + 25$	78057	(3)	3	-1	1	2	1	-1
4.0.74304.1	$x^4 - 2x^3 + 9x^2 - 8x + 10$	74304	(3)	4	1	1	4	1	1
4.0.62181.1	$x^4 - x^3 + 6x^2 - 16x + 25$	62181	(3)	4	1	1	4	1	1
4.0.48069.2	$x^4 - x^3 + 4x^2 + 6x + 15$	48069	(3)	4	1	1	4	1	1
4.0.94192.1	$x^4 + 12x^2 + 7$	94192	(3)	3	-1	1	2	1	-1

collection of data but we have run the same calculations on hundreds of non-Galois fields and for many more primes and always seen the same result.

We now look at similar data to examine the question whether the necessary condition is given in Proposition 3.3.4 is a sufficient condition for $\mathfrak{O}_K$ to admit a polarization of type $(1, p)$. It is not a sufficient condition. Interestingly, it was much more difficult to find counterexamples in this case than in the case of a Galois field. We were unable to find a primitive non-Galois CM-field K such that $\mathfrak{O}_K$ failed to admit a polarization of type $(1, 2)$ which also had any of the necessary values given in the above tables. I was, however, able to find a single field K for which $\mathfrak{O}_K$ fails to admit a polarization of type $(1, 3)$ but for which $r = 3$, $r' = 2$, $\left(\frac{\mathrm{Disc}_{K/\mathbb{Q}}}{3}\right) = \left(\frac{\mathrm{Disc}_{K_0^r/\mathbb{Q}}}{3}\right) = -1$, and $\left(\frac{\mathrm{Disc}_{K_0/\mathbb{Q}}}{3}\right) = \left(\frac{\mathrm{Disc}_{K^r/\mathbb{Q}}}{3}\right) = 1$.. This is the field labeled 4.0.65600.5 in the LMFDB which is generated over Q by a root of the polynomial $x^4 - 2x^3 + x^2 - 10x + 25$. Although this field does not have a polarization of type $(1, 3)$, there exists an ideal $\mathfrak{a}_p$ as given in Theorem 3.1.2. The nonexistence of a polarization was because the fractional ideal $\mathrm{Diff}_{K/\mathbb{Q}}\,\mathfrak{a}_p$ failed to be a principal fractional ideal. Again, as in the Galois case, this is expected for the same reasons, but it is interesting because it is so rare.

Chapter 5: Isomorphisms between polarized abelian varieties with CM

Recall that we have characterized in Theorem 3.1.2 how to construct an abelian surface with complex multiplication. It follows that if $(\Phi, \mathfrak{c}, \zeta)$ is a triple consisting of a CM-type Φ, a fractional ideal $\mathfrak{c}$ of K and an element $\zeta \in K$ such that $\zeta^{-1} \in K_\Phi(i\mathbb{R}_{>0})$ and $\zeta D_K^{-1}\mathfrak{c}^{-1}\overline{\mathfrak{c}}^{-1} \in R_m(K)$, this triple corresponds to a polarized abelian variety of type $(1, m)$ and the converse is also true. We want to use this to characterize when two polarized abelian varieties of type $(1, m)$ are isomorphic.

THEOREM 5.0.1. *Let Let K be a primitive quartic CM-field with CM-type Φ. Let m be a positive integer. Let $\mathfrak{c}_1$ and $\mathfrak{c}_2$ be fractional ideals of $\mathfrak{O}_K$. Let $\mathfrak{a}_1 = \prod_{p|m} \mathfrak{a}_{1,p}, \mathfrak{a}_2 = \prod_{p|m} \mathfrak{a}_{2,p} \in R_m(K)$ and ζ_1, ζ_2 be such that $\zeta_1^{-1}, \zeta_2^{-1} \in K_\Phi(i\mathbb{R}_{>0})$ and $(\zeta_1) = \mathfrak{c}\overline{\mathfrak{c}}D_K\mathfrak{a}_1$ and $(\zeta_2) = \mathfrak{c}\overline{\mathfrak{c}}D_K\mathfrak{a}_2$.*

Consider the polarizations induced by ζ_1 and ζ_2 respectively on $\mathbb{C}^2/\Phi(\mathfrak{c}_1)$ and $\mathbb{C}^2/\Phi(\mathfrak{c}_2)$. Denote these polarized abelian surfaces by A_1 and A_2 respectively. These are isomorphic as polarized abelian surfaces if and only if there exists $\gamma \in K, \gamma \neq 0$ such that

(1) $\mathfrak{c}_1 = \gamma\mathfrak{c}_2$ *and*
(2) $\zeta_1 = (\gamma\overline{\gamma})^{-1}\zeta_2$

Further, this is only possible if $\mathfrak{a}_{1,p} = \mathfrak{a}_{2,p}$ for each $p|m$.

PROOF. A proof is outlined in [**17**] during the proof of his Theorem 5.2. □

Once one has established this it is convenient to restate it in terms of the action of a certain group on the set of isomorphism classes of abelian surfaces with complex multiplication by $\mathfrak{O}_K$.

DEFINITION 5.0.2. Let I be the group of pairs $(\mathfrak{a}, \alpha)$ where $\mathfrak{a}$ is a fractional ideal of $\mathfrak{O}_K$ and α is a totally positive element of K_0 satisfying $\mathfrak{a}\overline{\mathfrak{a}} = (\alpha)$. Let P be the subgroup of pairs of the form $((x), x\overline{x})$ with x in $K^\times$. The quotient I/P is called the polarized class group of $\mathfrak{O}_K$, denoted $C(\mathfrak{O}_K)$.

With this definition in hand, we can produce other abelian surfaces with complex multiplication by K given that we already have one. We make a few more definitions for convenience:

DEFINITION 5.0.3. Let K be a primitive quartic CM-field. Φ be a CM-type on K. Let m be a positive integer.

(1) We denote by $\mathcal{A}(K, \Phi, m)$ the set of all isomorphism classes of polarized abelian surfaces with complex multiplication by K with a polarization of type $(1, m)$ and of CM-type Φ. If the CM-type Φ is already specified we may denote this set instead by $\mathcal{A}(K, m)$.

(2) Consider the set of all pairs of the form $(\mathfrak{c}, \zeta)$ with $\mathfrak{c}$ a fractional ideal of K and $\zeta \in K$ an imaginary element such that $\phi(\zeta)$ has positive imaginary part for each $\phi \in \Phi$ and such that $\zeta \mathfrak{c}^{-1}\overline{\mathfrak{c}}^{-1} \operatorname{Diff} K/\mathbb{Q}^{-1} \in R_m(K)$. We place upon this set an equivalence relation such that if $(\mathfrak{c}_1, \zeta_1)$ and $(\mathfrak{c}_2, \zeta_2)$ are two such pairs, we say $(\mathfrak{c}_1, \zeta_1) \sim (\mathfrak{c}_2, \zeta_2)$ when there exists $\gamma \in K$ such that the following two conditions are satisfied:
   (a) $\mathfrak{c}_1 = \gamma \mathfrak{c}_2$ and
   (b) $\zeta_1 = \gamma\overline{\gamma}\zeta_2$.
   We denote by $\mathcal{J}(K, \Phi, m)$ the set of equivalence classes of pairs under this equivalence relation.

(3) For each pair $(\mathfrak{c}, \zeta)$ in $\mathcal{J}(K, \Phi, m)$ there exists an ideal $\mathfrak{a} = \prod_{p|m} \mathfrak{a}_p$ in $R_m(K)$ such that $(\zeta) = \mathfrak{c}\overline{\mathfrak{c}} \prod_{p|m} \mathfrak{a}_p$. In other words, we have a map $\mathcal{J}(K, \Phi, m) \to R_m(K)$. Let $\mathfrak{a} = \prod_{p|m} \mathfrak{a}_p$ be in $\mathbb{R}_m(K)$. Denote by $\mathcal{J}(K, \Phi, m)_{\mathfrak{a}}$ the fiber of this map over $\mathfrak{a}$.

By Theorem 5.0.1 we have that $\mathcal{A}(K, \Phi, m)$ is in bijection with $\mathcal{J}(K, \Phi, m)$. The bijection is given by mapping a pair $(\mathfrak{c}, \zeta)$ to the abelian surface $\mathbb{C}^2/\Phi(\mathfrak{c})$ with the polarization $E : \Phi(\mathfrak{c}) \times \Phi(\mathfrak{c}) \to \mathbb{Z}$ given by $E(\Phi(x), \Phi(y)) = \operatorname{Tr}_{\mathbb{Q}}^{K}(\zeta^{-1}\overline{x}y)$ for all $x, y \in \mathfrak{c}$.

THEOREM 5.0.4. *Let K be a primitive quartic CM-field, Φ a CM-type on K and $\mathfrak{O}_K$ the ring of integers of K. There is an action of $C(\mathfrak{O}_K)$ on $\mathcal{J}(K, \Phi, m)$. If $(\mathfrak{a}, \alpha) \in C(\mathfrak{O}_K)$, this action on $(\mathfrak{c}, \zeta) \in \mathcal{J}(K, \Phi, m)$ is given by*

$$(\mathfrak{a}, \alpha) \cdot (\mathfrak{c}, \zeta) = (\mathfrak{a}\mathfrak{c}, \alpha\zeta).$$

PROOF. We must prove that this action is well-defined. By assumption, since $(\mathfrak{c}, \zeta)$ is in $\mathcal{J}(K, \Phi, m)$, the abelian surface it represents carries a polarization of type $(1, m)$ for some integer m and there exists by Theorem 3.1.2 some $\mathfrak{a} = \prod_{p|m} \mathfrak{a}_p \in R_m(K)$ such that

$$(\zeta) = \mathfrak{c}\overline{\mathfrak{c}} \operatorname{Diff}_{K/\mathbb{Q}} \prod_{p|m} \mathfrak{a}_p.$$

To show that the pair $(\alpha\mathfrak{c}, \alpha\overline{\alpha}\zeta)$ represents an abelian surface in $\mathcal{A}(K, \Phi, m)$, we first note that as α is real and totally positive, $\alpha\zeta$ is totally imaginary and the imaginary part of $\phi((\alpha\zeta)^{-1})$ has the same sign as $\phi(\zeta^{-1})$ so that $(\alpha\zeta)^{-1}$ is also in $K_\Phi(i\mathbb{R}_{>0})$. Now we have

$$(\alpha\zeta) = \mathfrak{a}\overline{\mathfrak{a}}(\zeta)$$

$$= \mathfrak{a}\mathfrak{c}\overline{\mathfrak{a}\mathfrak{c}}D_K \prod_{p|m} \mathfrak{a}_p.$$

This implies that $(\mathfrak{a}\mathfrak{c}, \alpha\zeta) \in \mathcal{J}(K, \Phi, m)$. So the action is well-defined. □

We wish to study the properties of this action. Is the action transitive? If it's not transitive, how many orbits do we have? It is apparent from the proof that the action is defined that we cannot possibly map one triple to another if the ideal $\prod_{P|m} \mathfrak{a}_p$ associated with each polarization are different, in other words the action descends to an action on the fibers $\mathcal{J}(K, \Phi, m)_f a$ so the action can only be transitive if there is only one such collection $fa \in R_m(K)$ giving rise to a polarization. And so in order to answer this we need to find how many different collections $(\mathfrak{a}_p)$ are possible. We have not yet found a good way to measure how many possibilities there are. However this does prove a nice theorem to end on in some restricted conditions.

THEOREM 5.0.5. *Let K be a primitive quartic CM-field, Φ a CM-type on K and $\mathfrak{O}_K$ the ring of integers of K. The action of $C(\mathfrak{O}_K)$ on $J(K, \Phi, m)$ is transitive if and only if $R_m(K)$ is a singleton.*

Bibliography

1. Dummit, David and Foote, Richard, *Abstract Algebra, 3rd ed.* John Wiley and Sons, 2004.
2. Edgar, Hugh and Peterson, Brian *Some Contributions to the Theory of Cyclic Quartic Extensions of the Rationals* Journal of Number Theory, Volume 12, Issue 1, 1980.
3. Freitag, Eberhard *Complex Analysis 2*. Springer-Verlag, 2011.
4. Hasse, Helmut *Number Theory*. Springer-Verlag, 1980.
5. Igusa, Junichi. *Theta Functions*, Springer-Verlag, 1972.
6. Lang, Serge *Abelian Varieties*, Springer-Verlag, 1983.
7. Marcus, Daniel A. *Number Fields, Second Edition* Springer-Verglag, 2018.
8. Mumford, David *Abelian Varieties*, Hindustan Book Agency, 2008
9. Narciewicz, Wladyslaw *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, 2004
10. Neukirch, Jürgen *Algebraic Number Theory*. Springer-Verlag, 2013.
11. Rotman, Joseph *An Introduction to the Theory of Groups*. Springer-Verlag, 1995.
12. Shalit, Ehud De and Goren, Eyal Z. *On Special values of theta functions of genus two*, Annales de l'Institut Fourier, 775-799, Association des Annales de l'institut Fourier, volume 47, number 3, 1997, http://www.numdam.org/articles/10.5802/aif.1580/.
13. Shimura, Goro. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998.
14. Shimura, Goro. *Arithmetic of Alternating Forms and Quaternion Hermitian Forms*. Journal of the Mathematical Society of Japan, Mathematical Society of Japan, volume 15, number 1, 1963, https://doi.org/10.2969/jmsj/0151003.
15. Silverman, Joseph *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.
16. Spallek, Anne-Monika, *Kurven vom Geschlecht 2 und ihreAnwendung in Public-Key-Kryptosystemen* P.h.D.Thesis, Universität Gesamthochschule Essen
17. Streng, Marco, *Complex Multiplication of Abelian Surfaces* Ph.D. Thesis, Universiteit Leiden, 2010
18. Washington, Lawrence *Introduction to Cyclotomic Fields*. Springer-Verlag, 1997.